ТЕХНОЛОГИЧЕСКАЯ ИНСТРУКЦИЯ ПО ПОДКЛЮЧЕНИЮ К ПОДСИСТЕМЕ БЮДЖЕТНОГО ПЛАНИРОВАНИЯ ГОСУДАРСТВЕННОЙ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОБЩЕСТВЕННЫМИ ФИНАНСАМИ «ЭЛЕКТРОННЫЙ БЮДЖЕТ» С ИСПОЛЬЗОВАНИЕМ КВАЛИФИЦИРОВАННОЙ ЭЛЕКТРОННОЙ ПОДПИСИ

МОСКВА

АННОТАЦИЯ

Настоящий документ является инструкцией по защищенному удаленному подключению пользователей к подсистеме бюджетного планирования государственной интегрированной информационной системы управления общественными финансами «Электронный бюджет» (далее – Система) с использованием квалифицированной электронной подписи.

СОДЕРЖАНИЕ

1. TP	ЕБОВАНИЯ К АППАРАТНО-ТЕХНИЧЕСКИМ И ПРОГРАММНЫМ СРЕДСТВАМ	4
1.1.	ТРЕБОВАНИЯ К ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ	4
1.2.	ТРЕБОВАНИЯ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ	4
1.3.	Настройка программного обеспечения	4
1.3.1.	. Установка криптопровайдера «КриптоПро CSP»	4
1.3.2.	. Установка драйвера используемого носителя ключевой информации сертификата	
польз	зователя	6
1.3.3.	. Установка личного сертификата и сертификата доверенного корневого центра	
серти	ификации	12
1.3.4.	. Настройка Internet Explorer	21
2. BX	КОД ПОДСИСТЕМУ БЮДЖЕТНОГО ПЛАНИРОВАНИЯ ГОСУДАРСТВЕННОЙ	
ИНТІ	ЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОБЩЕСТВЕНН	ЫМИ
ФИН	ІАНСАМИ «ЭЛЕКТРОННЫЙ БЮДЖЕТ»	24
3. ПР	РОБЛЕММЫ ПРИ ПОДКЛЮЧЕНИИ К СИСТЕМЕ И ИХ УСТРАНЕНИЕ	27
3.1.	ПРОБЛЕМА С СЕРТИФИКАТОМ БЕЗОПАСНОСТИ	27
3.2.	Вставьте ключевой носитель	27
3.3.	НЕ УДАЕТСЯ ОТОБРАЗИТЬ ЭТУ СТРАНИЦУ	28
3.4.	403 Access Denied	29
3.5.	НЕ УДАЕТСЯ ОТОБРАЗИТЬ ЭТУ СТРАНИЦУ. ВКЛЮЧИТЕ ПРОТОКОЛЫ TLS	29
3.6.	Иные ошибки	31

1. ТРЕБОВАНИЯ К АППАРАТНО-ТЕХНИЧЕСКИМ И ПРОГРАММНЫМ СРЕДСТВАМ

1.1. Требования к техническому обеспечению

Для автоматизированных рабочих мест пользователей Системы устанавливаются следующие минимальные технические требования:

1) Процессор с тактовой частотой не менее 600 МГц;

2) Объем оперативной памяти не менее 128 Мб;

3) Объем жесткого диска не менее 10 Гб;

4) Клавиатура;

5) Монитор SVGA (графический режим должен иметь разрешение не менее 1024х768);

6) USB-порт;

7) Квалифицированный сертификат ключа проверки электронной подписи (может быть предоставлен на носителях ruToken CSP, eToken CSP);

8) Манипулятор типа мышь.

На рабочем месте должен быть предоставлен доступ к сети Интернет со скоростью не менее 256 Кбит/сек.

1.2. Требования к программному обеспечению

Программные средства, требуемые для обеспечения возможности подписания документов электронной подписью:

1) Интернет-браузер «Internet Explorer» версия 10.0 и выше;

2) Операционная система Windows XP и выше;

3) Сертифицированная версия «КриптоПро CSP» - криптопровайдер, вспомогательная программа, использующаяся для генерации электронных подписей, работы с сертификатами и т.д.

1.3. Настройка программного обеспечения

1.3.1. Установка криптопровайдера «КриптоПро CSP»

 1. Загрузите и запустите установочный файл сертифицированной версии «КриптоПро
 СSP»,
 доступный
 на
 странице

 https://www.cryptopro.ru/products/csp/downloads.
 Окно
 приветствия
 установщика

 «КриптоПро CSP»
 представлено на рисунке (Рисунок 1).
 Ски
 Ски
 Ски

N	УриптоПро CSP 3.9.8227	×
	КРИПТО-ПРО - ключевое слово в защите информации http://www.cryptopro.ru Благодарим за выбор КриптоПро CSP. Для быстрой установки нажмите "Установить". Если необходимы расширенные настройки, нажмите "Опции". Продолжая установку, вы принимаете условия Лицензионного соглашения.	
	Опции Установить Отмена	

Рисунок 1. Окно приветствия «КриптоПРО CSP»

2. Нажмите кнопку «Установить». После завершения процесса установки и настройки «КриптоПРО CSP» появится сообщение об успешной установке (Рисунок 2).

КриптоПро CSP	×
КриптоПро CSP успешно у	становлен.
	ОК

Рисунок 2. Установка «КриптоПро CSP»

При установке программы «КриптоПро CSP» может быть запрошен лицензионный ключ, который поставляется с установочным пакетом «КриптоПро CSP».

3. Запустите «КриптоПро СSP» (Пуск/Все программы/КриптоПро/КриптоПро СSP). Откройте вкладку «Настройки TLS» и приведите настройки программы в соответствие с Рисунок 3 (для перенастройки могут потребоваться права администратора на локальном компьютере и перезагрузка компьютера).

КриптоПро	CSP		— ×
Общие	Оборудование	Сервис	Дополнительно
Алгоритмы	Безопасность	Winlogon	Настройки TLS
Клиент —			
Использ	овать протокол OCSP		
M He Hpos	ерять сертификат сер	вера на отзыв	
И Не пров	ерять назначение собс	твенного серти	фиката
📃 Не испо	льзовать устаревшие с	tipher suite-ы	
Сервер			
Использ	овать протокол OCSP		
🔽 Не пров	ерять сертификат кли	ента на отзыв	
Не проверять назначение собственного сертификата			
🔲 Не использовать устаревшие cipher suite-ы			
Поддерживать RFC 5746 (Renegotiation Indication)			
🔲 Требова	ать поддержку RFC 574	46 (Renegotiation	n Indication)
Использ	ювать сертификат ком	пьютера по умо	лчанию
Размер	кэша сессий:		64 🌲
Максима	альное число ЦС в запр	осе сертифика	ra: 100 🚔
L			
	ОК	Отме	на Применить

Рисунок 3. Настройки TLS

1.3.2. Установка драйвера используемого носителя ключевой информации сертификата пользователя

Если в качестве носителя ключевой информации сертификата пользователя используется носитель типа eToken или Rutoken, необходимо выполнить установку драйвера соответствующего накопителя в ОС (если ранее не был установлен).

Если необходимый драйвер не установлен, необходимо:

а) Драйвер носителя типа Rutoken

1. Загрузите и запустите установочный файл, доступный на странице <u>http://www.rutoken.ru/support/download/drivers-for-windows/</u>. Окно приветствия установщика драйверов Rutoken представлено на рисунке (Рисунок 4).





2. Нажмите кнопку «Далее». На экране отобразится диалог о готовности к выполнению установки драйверов (Рисунок 5).

🛃 Драйверы Rutoken	X
Программа готова к установке Драйверов Rutoken	рутокен [®]
Нажмите кнопку "Установить", чтобы начать установку.	
Нажмите кнопку "Отмена" для выхода из программы.	
InstallShield	
< <u>Н</u> азад Устано	вить Отмена

Рисунок 5. Сообщение о готовности к выполнению установки драйверов

3. Нажмите кнопку «Установить». Начнется установка драйверов Rutoken на APM пользователя. Установка может занять несколько минут, информация о прогрессе установки выводится в окне, представленном на рисунке (Рисунок 6).

闄 Драйвер	ы Rutoken		
Установі	ка Драйверов Rutoken		рутокен ®
**	Пожалуйста, дождитесь око Это может занять несколько	нчания установки Дра минут.	йверов Rutoken.
	Состояние установки:		
InstallShield –	[< <u>Н</u> азад <u>Д</u> а	anee >



После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 7).



Рисунок 7. Сообщение об успешной установке драйверов Rutoken.

4. Нажмите кнопку «Готово». Окно установщика драйверов Rutoken будет закрыто.

5. В случае появления диалога о необходимости перезагрузки автоматизированного рабочего места Пользователя, ответить отрицательно.

b) Драйвер носителя типа eToken

1. Загрузите и запустите установочный файл, доступный на странице <u>http://www.aladdin-rd.ru/support/downloads/etoken/</u>. Окно приветствия установщика драйвера eToken представлено на рисунке (Рисунок 8).





2. Нажмите кнопку «Next». На экране появится диалог выбора языка, который будет использован в устанавливаемом ПО (Рисунок 9).

🛃 eToken PKI Client 5.1 SP1 Setup	
	Ready to Install the Application Select the language for eToken PKI Client.
Select eToken PKI Client interface language English	
Clic	k Next to begin installation.
	< <u>B</u> ack Next > Cancel

Рисунок 9. Окно выбора языка программы, управляющей ключевыми носителями eToken

3. Так как для решения задач, возникающих при работе в системе «Электронный бюджет», данное ПО не будет использоваться пользователями системы, то выбор языка можно пропустить, нажав кнопку «Next». На экране появится диалог лицензионное соглашение (Рисунок 10).

😸 eToken PKI Client 5.1 SP1 Setup	
Find-User License Agreemen Please read the following license a	t agreement carefully.
ALADDIN KNOWLEDGE SYSTEMS LTD. eTOKEN ENTERPRISE END USER LICENSE AGREI	EMENT
IMPORTANT INFORMATION - PLEASE READ THIS AC CAREFULLY BEFORE OPENING THE PACKAGE AND/ THE CONTENTS THEREOF AND/OR BEFORE DOWNLO INSTALLING THE SOFTWARE PROGRAM. ALL ORDERS USE OF THE eTOKEN ENTERPRISE PRODUCTS (inclu limitation, libraries, utilities, diskettes, CD-ROM, eToken [™] ko accompanying technical documentation) (hereinafter "Product")	GREEMENT OR USING ADING OR FOR AND ding without eys and the SUPPLIED
< Back Next >	Cancel

Рисунок 10. Окно просмотра лицензионного соглашения

4. Выберете пункт «I accept the license agreement» и нажмите кнопку «Next». На экране появится диалог выбора пути установки компонентов устанавливаемого ПО (Рисунок 11).

B eToken PKI Client 5.1 SP1 Setup
Destination Folder Select a folder where the application will be installed.
Setup will install the eToken PKI Client 5.1 SP1 files in the following folder. To install in a different folder, click Browse and navigate to the required folder. You can choose not to install eToken PKI Client 5.1 SP1 by clicking Cancel to exit the Setup.
Destination Folder C:\Program Files\Aladdin\eToken\ Browse
< <u>B</u> ack Next > Cancel

Рисунок 11. Окно выбора пути для установки программы

5. Оставьте путь установки по умолчанию либо измените на необходимый. Нажмите кнопку «Next».

Начнется установка программы и драйверов. Диалог процесса установки представлено на рисунке (Рисунок 12).

🗒 eToken PKI Client 5.1 SP1 Setup	
eToken Updat Your key to esecurity	ing System lected features are being installed.
Copying new files File: aksup.inf Directory: C:\Windows\system32\Set Size: 4545	up\Aladdin\eToken\
Time remaining: 6 seconds	
	Cancel

Рисунок 12. Прогресс установки драйверов eToken

После завершения установки пользователю будет выведено сообщение об успешной установке драйверов, представленное на рисунке (Рисунок 13).



Рисунок 13. Сообщение об успешной установке драйверов Rutoken

6. Нажмите кнопку «Finish». Окно установщика драйверов будет закрыто.

7. В случае появления диалога о необходимости перезагрузки автоматизированного рабочего места пользователя, ответить отрицательно.

1.3.3. Установка личного сертификата и сертификата доверенного корневого центра сертификации

Установка сертификата пользователя и доверенного корневого центра сертификации выполняется под учетной записью пользователя, которая будет использоваться в процессе входа в личный кабинет системы «Электронный бюджет».

Для добавления сертификатов:

 1. Запустите
 «КриптоПро
 СSP»
 (Пуск/Все

 программы/КриптоПро/КриптоПро
 СSP).
 В открывшемся окне на вкладке

 «Сервис» необходимо нажать на кнопку «Просмотреть сертификаты в контейнере»
 (Рисунок 14).



Рисунок 14. Добавление ключа в хранилище

2. В открывшемся диалоговом окне «Сертификаты в контейнере закрытого ключа» нажмите на кнопку «Обзор» и выберите используемый ключ (предварительно установленный в USB-порт или дисковод ключ, предоставленный на носителе ruToken/eToken") (Рисунок 15). После этого нажмите на кнопку «OK».

🖻 Ce	ртификаты в контейнере закрытого ключа	C X
Ko	нтейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере	
Имяк	лючевого контейнера:	Обзор
Введ	енное имя задает ключевой контейнер: По о КриптоПро CSP	ертификату
Выбе	0:09:52 Выбор ключевого контейнера В списке показывать:	
	Список ключевых контейнеров пользователя: Считыватель Имя контейнера	Отмена
	AKS ifdh 0 7b061ab6-d6a6-4acc-8780-b07ad0aefd84	
	ОК Отмена	

Рисунок 15. Выбор ключевого контейнера

3. Для завершения выбора контейнера закрытого ключа нажмите кнопку «Далее» (Рисунок 16)

腔 Сертификаты в контейнере закрытого ключа
Контейнер закрытого ключа Введите или укажите контейнер закрытого ключа для просмотра сертификатов в этом контейнере
<u>Имя ключевого контейнера:</u> 76061ab6-d6a6-4acc-8780-b07ad0aefd84
Введенное имя задает ключевой контейнер:
Выберите CSP для поиска ключевых контейнеров: Crypto-Pro GOST R. 34. 10-2001 Cryptographic Service Provider
< <u>Н</u> азад Далее > Отмена

Рисунок 16. Выбор контейнера закрытого ключа

4. В открывшемся диалоговом окне нажмите на кнопку «Установить» (Рисунок 17):

⊵ Сертификаты в контейнере закрытого ключа				
Сертификат для просмотра Просмотрите и выберите сертификат				
Сертификат:				
С <u>у</u> бъект:	СНИЛС=	ОГРН=1037739085636, ИНН=007710168360, T=		
Поставщик:	STREET ="127287, г. Москва, Старый Петровско-Разумовский проезд, 22 апреля 2015 г. 17:39:18 22 апреля 2016 г. 17:39:18 0 1D0 7D09 47EB AE70 0000 004D 0006 0002			
Действителен <u>с</u> :				
Действителен <u>п</u> о:				
Серийный <u>н</u> омер:				
		<u>У</u> становить С <u>в</u> ойства О <u>б</u> зор		
		< Назад Готово Отмена		

Рисунок 17. Выбор сертификата

5. После установки появится уведомление об успешной установке сертификата. Для подтверждения нажмите кнопку «ОК» (Рисунок 18).



Рисунок 18. Уведомление об успешной установке сертификата

Если в процессе выполнения действий появится сообщение «A new certificate was added to the certificate store» (Рисунок 19), необходимо нажать кнопку «Cancel».

😑 eToken Certificate Import 🧮 🎫				
1	A new certificate was added to the certificate store. Click OK to add this certificate to eToken.			
	OK Cancel			

Рисунок 19. Сообщение драйвера eToken

6. Для установки сертификата доверенного корневого центра сертификации нажмите кнопку «Свойства» в окне выбора сертификата (Рисунок 17).

7. В открывшемся окне перейдите на вкладку «Путь сертификации» (Рисунок 20).

8. Проверьте, установлен ли сертификат верхнего уровня (сертификат доверенного корневого центра сертификации).

Знак (1) 🐷 свидетельствует о том, что сертификат не установлен.

Знак (2) 👎 свидетельствует о том, что сертификат установлен.

Если у первого в списке сертификата стоит знак 1, то нажатием левой кнопки мыши выберите данный сертификат.

Если у первого в списке сертификата стоит знак 2, переходите к шагу 22 раздела 1.3.2 данной инструкции.

Сертификат				
Общие Состав Путь сертификации				
Путь сертификации				
<mark>Бар УЦ ИИТ (КЗ)</mark> Минфин России				
Просмотр сертификата				
Состояние сертификата:				
Этот сертификат содержит недействительную цифровую подпись.				
, Подробнее о <u>путях сертификации</u>				
ок				

Рисунок 20. Сертификат. Путь сертификации

9. После выбора сертификата, нажмите на кнопку «Просмотр сертификата». В открывшемся окне перейдите на вкладку «Состав» и нажмите на кнопку «Копировать в файл...» (Рисунок 21)

ертификат					
Общие Состав Путь сертификации					
Deveren a la Constantina					
Поле	Значение	*			
📴 Версия	V3	-			
📴 Серийный номер	01 cf a2 68 e4 66 1e b0 00 00	-			
🛅 Алгоритм подписи	1.2.643.2.2.3				
🛄 Издатель	УЦ ИИТ (КЗ), ОАО "ИнфоТеК				
🛅 Действителен с	18 июля 2014г. 12:16:00				
🛄 Действителен по	18 июля 2020 г. 12:16:00				
Субъект	УЦ ИИТ (КЗ), ОАО "ИнфоТеК	-			
ПП Открытый ключ	1 2 643 2 2 19 (N Rite)				
<u>С</u> войства <u>К</u> опировать в файл Подробнее о <u>составе сертификата</u>					
	Of	(

Рисунок 21. Копирование сертификата в файл

10. В открывшемся мастере экспорта сертификатов нажмите на кнопку «Далее».

11. Убедитесь, что в открывшемся окне выбора формата экспортируемого сертификата выбран только вариант «Файлы X.509 (.CER) в кодировке DER, затем нажмите кнопку «Далее».

12. В окне «Имя экспортируемого файла» нажмите кнопку «Обзор».

13. В диалоговом окне «Сохранить как» перейдите в папку «Рабочий стол», в поле «Имя файла» укажите «Сертификат для ЭБ», нажмите кнопку «Сохранить».

14. Убедитесь, что в окне «Имя экспортируемого файла» в поле «Имя файла» верно отобразился путь сохранения сертификата (например, C:\Users\0990\Desktop\Ceptuфикат для ЭБ.cer). Нажмите кнопку «Далее».

15. Подтвердите успешный экспорт сертификата, нажав кнопку «ОК».

16. В окне «Завершение работы мастера экспорта сертификатов» нажмите кнопку «Готово»

17. Перейдите в папку «Рабочий стол», найдите и откройте файл «Сертификат для ЭБ.cer».

18. В появившемся окне нажмите на кнопку «Установить сертификат» (Рисунок 22). На экране отобразится мастер импорта сертификатов, где необходимо нажать кнопку «Далее».

Сертификат		
Общие Состав Путь сертификации		
Сведения о сертификате		
Нет доверия к этому корневому сертификату центра сертификации. Чтобы включить доверие, установите этот сертификат в хранилище доверенных корневых сертификатов центров сертификации.		
Кому выдан: УЦ ИИТ (К 1)		
Кем выдан: УЦ ИИТ (К 1)		
Действителен с 22. 04. 2015 по 22. 04. 2021		
Установить сертификат Заявление поставщика Подробнее о сертификатах		
ОК		

Рисунок 22. Установка корневого сертификата центра сертификации

19. В окне «Хранилище сертификата» (Рисунок 23) выбрать размещение сертификата вручную, указав поле «Поместить сертификаты в следующее хранилище». Нажать кнопку «Обзор...».

Хранилиц	це сертификатов
Храни храня	ілища сертификатов - это системные области, в которых атся сертификаты.
Выбо можно	р хранилища может быть произведен Windows автоматически, или же о указать размещение сертификата вручную.
0	Автоматически выбрать хранилище на основе типа сертификата
۲	Поместить все сертификаты в следующее хранилище
	Хранилище сертификатов:
	<u></u> бзор
Подробне	е о <u>хранилищах сертификатов</u>

Рисунок 23. Выбор хранилища сертификата

20. В окне выбора хранилища сертификатов выберите контейнер «Доверенные корневые центры сертификации». Нажмите кнопку «Ок» (Ошибка! Источник ссылки не найден.).

Выбор хранилища сертификата			
Выберите <u>х</u> ранилище сертификатов.			
Личное Доверенные корневые центры сертис Доверительные отношения в предпри Промежуточные центры сертификаци Доверенные издатели Сертификаты к которым нет доверис Ш			
Показать физические хранилища ОК Отмена			

Рисунок 24. Выбор хранилища сертификата

21. В окне «Мастер импорта сертификатов» нажмите кнопку «Далее» затем кнопку «Готово». В случае успешного импорта сертификата отобразится диалог

«Импорт успешно выполнен», где необходимо нажать кнопку «ОК». Если появится окно «Предупреждение безопасности» нажмите кнопку «Да».

22. Убедитесь, что личный сертификат с наименованием, аналогичным тому, что было указано в поле «Сертификат» на Рисунок 17, успешно установлен в директории «Сертификаты–текущий пользователь – Личное – Реестр – Сертификаты». Для этого запустите утилиту «Сертификаты» расположенную в «Пуск/Все программы/КриптоПро/Сертификаты» и найдите данный сертификат в директории «Сертификаты–текущий пользователь – Личное – Реестр – Сертификаты» (Рисунок 25).

🗃 Сертификаты				
🗐 Файл Действие Вид Окно Справка				
🗢 🔿 🗾 📋 🙆 😹 🛛 🖬				
📔 Корень консоли	Кому выдан	Кем выдан	Срок действия	
 Дертификаты - текущий пользователь Личное 	🛱 Громова Елена Александровна	УЦ ИИТ (КЗ)	22.04.2016	
⊿ ² Реестр ² Сертификаты				
 Доверенные корневые центры сертификации Доверительные отношения в предприятии Промеходошные центры сертификации 				
 Промежуючные центры сертификации Объект пользователя Active Directory Ловеренные издатели 				
 Сертификаты, к которым нет доверия Сторонние корневые центры сертификации 				
▷ Consepentue лица ▷ Consepentue заявок на сертификат				
 Доверенные корневые сертификаты смарт-карты Г Доверенные (локальный компьютер) 				
	•		•	
Хранилище Реестр содержит 1 сертификат.				

Рисунок 25. Утилита «Сертификаты»

23. Если сертификат отсутствует, вернитесь к шагу 4, нажмите кнопку «Свойства» и установите сертификат, следуя шагам 18-21 раздела 1.3.2 данной инструкции, выбрав на шаге 20 контейнер «Личное».

24. Если сертификат присутствует, откройте его. Перейдите на вкладку «Путь сертификации» и проверьте, установлен ли сертификат доверенного корневого центра сертификации в соответствии с шагом 8 раздела 1.3.2 данной инструкции. Если сертификат установлен, то автоматизированное рабочее место пользователя успешно настроено для работы с Системой.

1.3.4. Настройка Internet Explorer

- 1. Открыть свойства веб-обозревателя Internet Explorer.
- 2. Перейти на вкладку «Безопасность».

Содоржание	Descriptions			
Содержание	Гюдключе		рограммы	дополнительно
Оощие	DESON		Конф	иденциальность
Зыберите зону, Оранования Интернет	для настройки е	е параметро Инадежные сайты	з безопасност Опасные сайты	ти.
Надех	кные сайты		ſ	C-*
Зона для надежных сайтов, которые не причинят вреда вашему компьютеру или данным. В этой зоне есть веб-сайты. Уровень <u>б</u> езопасности для этой зоны				
Разрешенны	е уровни: любы	e		
Средний Запрос перед загрузкой опасного содержимого - Неподписанные элементы ActiveX не загружаются - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -				
Включить защищенный режим (потребуется перезапуск Internet Explorer)				
Дру <u>г</u> ой По умолчанию				
Выбрать уровень безопасности по умолчанию для всех зон				

Рисунок 26. Диалог настройки безопасности браузера

- 3. Выбрать зону для настройки «Надежные узлы» (Рисунок 26).
- 4. Нажать кнопку «Сайты».

Надежные сайты	X	
Вы можете добавлять в эту зону веб-сайты из нее. Заданные для зоны параметры безог использоваться для всех ее сайтов.	и удалять их асности будут	
Добавить в зону следующий узел:		
https://ssl.budgetplan.minfin.ru	Добавить	
<u>В</u> еб-сайты:		
	<u>У</u> далить	
☑ Для всех сайтов этой зоны требуется проверка серверов (https:)		
	<u>З</u> акрыть	

Рисунок 27. Диалог настройки доверенных узлов.

5. В поле «Добавить в зону следующий узел» задать значение «https://ssl.budgetplan.minfin.ru/» и нажать кнопку «Добавить» (Рисунок 27).

- 6. В окне «Надежные сайты» нажать кнопку «Закрыть».
- 7. В окне «Свойства браузера» нажать кнопку «ОК».

2. ВХОД ПОДСИСТЕМУ БЮДЖЕТНОГО ПЛАНИРОВАНИЯ ГОСУДАРСТВЕННОЙ ИНТЕГРИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОБЩЕСТВЕННЫМИ ФИНАНСАМИ «ЭЛЕКТРОННЫЙ БЮДЖЕТ»

1. Для входа в Систему необходимо запустить интернет браузер «Internet Explorer» и в адресной строке ввести http://budget.gov.ru/lk (Рисунок 28).



Рисунок 28. Единый портал бюджетной системы

2. На странице Единого портала бюджетной системы нажмите на кнопку «Переход к подсистеме «Бюджетное планирование».

3. После нажатия на кнопку браузер осуществит перенаправление по адресу https://ssl.budgetplan.minfin.ru/http/BudgetPlan/. Если перенаправление не произошло, введите указанную ссылку в адресную строку браузера.

4. В появившемся окне, нажмите на кнопку «Вход по сертификату» (Рисунок 29).



Рисунок 29. Окно выбора вида входа в систему

5. После выбора метода аутентификации «Вход по сертификату», Система автоматически запрашивается сертификат ключа проверки электронной подписи и пин-код сертификата, затем осуществляется поиск пользователя-владельца сертификата и происходит открытие главного окна Системы.

Если различные пользователи используют для авторизации один сертификат (например, одно уполномоченное лицо имеет различные роли), то Система предложит выбрать конкретного пользователя (Рисунок 30). После выбора логина, необходимо нажать кнопку «Войти».



Рисунок 30. Окно выбора логина пользователя

3. ПРОБЛЕММЫ ПРИ ПОДКЛЮЧЕНИИ К СИСТЕМЕ И ИХ УСТРАНЕНИЕ

3.1. Проблема с сертификатом безопасности

Если между шагами 3 и 4 раздела 2 данной инструкции появляется сообщение «Возникла проблема с сертификатом безопасности этого веб-сайта» (Рисунок 31), необходимо нажать на кнопку «Продолжить открытие веб-сайта (не рекомендуется)».

8	Возникла проблема с сертификатом безопасности этого веб-сайта.
	Сертификат безопасности этого веб-сайта не был выпущен доверенным центром сертификации. Срок действия сертификата безопасности этого веб-сайта истек или еще не начинался. Сертификат безопасности этого веб-сайта был выпущен для веб-сайта с другим адресом.
	Наличие ошибок в сертификате безопасности может указывать на попытку обмана или перехвата данных, которые вы отправляете на сервер.
	Мы рекомендуем вам закрыть эту веб-страницу и не работать с данным веб-сайтом.
	🥙 Щелкните здесь, чтобы закрыть эту веб-страницу.
	😵 Продолжить открытие этого веб-сайта (не рекомендуется).
	🕞 Подробнее

Рисунок 31. Проблема с сертификатом безопасности

3.2. Вставьте ключевой носитель

Если между шагами 3 и 4 раздела 2 данной инструкции появляется сообщение КриптоПРО CSP «Вставьте ключевой носитель» (Рисунок 32), необходимо:

- 1. Установить установите в рабочий USB-порт автоматизированного рабочего места пользователя Системы, предоставленный на носителе ruToken/eToken.
- 2. Перезапустите браузер Internet Explorer.
- 3. Повторите шаги раздела 2 данной инструкции.

КриптоПро CSP	×			
0:09:47 Вставьте ключевой носитель "ETOKEN_PRO_27373809180c".				
Сведения				
Устройства:	Вставленный носитель:			
	Состояние: Отсутствует носитель.			
AKS ifdh 1				
	Отмена Сведения <<			

Рисунок 32. Вставьте ключевой носитель

3.3. Не удается отобразить эту страницу

🗲 🕣 🎑 https://ssl.budgetplan.minfin.ru/http/BL 🔎 🕆 🖒 🥔 Не удается отоб	іразить эту 🗙 🔐 🔐
Файл Правка Вид Избранное Сервис Справка	Не удается отобразить эту страницу
	https://ssi.budgetplan.minfin.ru/http/Budge
Не удается отоб страницу - Убедитесь, что веб-адрес https://ssl.budgetpla - Найдите страницу с помощью поисковой сисс - Обновите страницу через несколько минут.	разить эту n.minfin.ru правильный. темы.
<	>

Рисунок 33. Не удается отобразить эту страницу

Если появляется сообщение об ошибке «Не удается отобразить эту страницу» (Рисунок 33), необходимо:

1. Проверить версию браузера Internet Explorer (версия должна быть не ниже Internet Explorer 10) при необходимости обновите. Для проверки версии:

откройте браузер Internet Explorer;

в меню «Справка» нажмите левой клавишей мыши на кнопку «О программе» (Рисунок 34) откроется окно «О программе», где будет указана текущая версия браузера Internet Explorer.

Справка					
	Справка Internet Explorer F1				
	Новые возможности Internet Explorer 11 Техническая поддержка				
	О программе				
Р	NFENDOTO ROT	Т			

Рисунок 34. О программе

2. Проверить, установлен ли криптопровайдер «КриптоПРО CSP», в случае отсутствия установить (см. раздел 1.3.1. данной инструкции).

3. Проверить настройки «КриптоПРО CSP» (см. шаг 3. раздела 1.3.1. данной инструкции).

3.4. 403 Access Denied

В случае возникновения ошибки «403 Access Denied» (Рисунок 35), необходимо в соответствии с шагами 6-17 раздела 1.3.3. данной инструкции сохранить сертификат корневого центра сертификации, заархивировать его (обязательно!) и отправить его на адрес электронной почты <u>0990@minfin.ru</u> с указанием, наименования учреждения, ФИО пользователя и логина в Системе.



Рисунок 35. 403 Access Denied

3.5. Не удается отобразить эту страницу. Включите протоколы TLS

Если появляется сообщение об ошибке «Не удается отобразить эту страницу» (Рисунок 36), необходимо:

Файл Правка Вид Избранное Сервис Справка

Не удается отобразить эту страницу

Включите протоколы TLS 1.0, TLS 1.1 и TLS 1.2 в разделе "Дополнительные параметры" и снова попробуйте подключиться к веб-странице **https://ssl.budgetplan.minfin.ru**. Если не удается устранить ошибку, обратитесь к администратору веб-сайта.

0-0

e Не удается отобр

Изменить параметры

Рисунок 36. Не удается отобразить эту страницу. Включите протоколы TLS

1. Проверить версию браузера Internet Explorer (версия должна быть не ниже Internet Explorer 10) при необходимости обновите. Для проверки версии:

откройте браузер Internet Explorer;

в меню «Справка» нажмите левой клавишей мыши на кнопку «О программе» (Рисунок 34) откроется окно «О программе», где будет указана текущая версия браузера Internet Explorer.

Справка					
	Справка Internet Explorer F1				
	Новые возможности Internet Explorer 11 Техническая поддержка				
	О программе				
Р	TCA OTODDAR	ИŤ			

Рисунок 37. О программе

2. Проверить, установлен ли криптопровайдер «КриптоПРО CSP», в случае отсутствия установить (см. раздел 1.3.1. данной инструкции).

3. Проверить настройки «КриптоПРО CSP» (см. шаг 3. раздела 1.3.1. данной инструкции).

4. Проверить настройки браузера Internet Explorer. Для проверки настроек браузера:

откройте браузер Internet Explorer;

в меню «Сервис» нажмите левой клавишей мыши на кнопку «Свойства браузера» или «Свойства обозревателя»;

в появившемся окне откройте вкладку «Дополнительно» и сверьте настройки с Рисунок 38.

Свойства браузера						
Общие	Безопасность	Ko	нфиденциальность			
Содержание	Подключения	Программы	Дополнительно			
Параметры						
🔒 Безопас	🔒 Безопасность 🔺					
SSL	2.0		-			
SSL	3.0					
V TLS	1.0					
Бло	ировать небезопасные	рисунки и друго	й смешанн			
ВКЛ	очить внутреннюю под	держку хмснтт	*			
	очить расширенный защ	ищенный режим и рар*				
И ВКЛ	очить фильтр SmartScre	en l				
🗸 Вкл	очить хранилище DOM					
✓ Испе	льзовать TLS 1.1					
🗹 Исп	льзовать TLS 1.2					
E He d	охранять зашифрованны	ые страницы на ,	диск			
Οτη	🔽 Отправлять на посещаемые через Internet Explorer ве 🍸					
•						
* Изменения	будут применены после	перезапуска ко	мпьютера			
	Восстановить д	ополнительные	параметры			
Сброс параметр	юв настройки Internet E	xplorer				
Возвращает параметры Internet Explorer к значениям Сброс						
Используйте сброс только если обозреватель неработоспособен.						
· · · · · · · · · · · · · · · · · · ·						
ОК Отмена Применить						

Рисунок 38. Вкладка "Дополнительно"

3.6. Иные ошибки

В случае возникновения ошибок в процессе подключения и настройки программного обеспечения, не описанных в данной инструкции, необходимо:

сделать снимок экрана (скриншот) ошибки;

в соответствии с шагами 6-17 раздела 1.3.3. инструкции сохранить сертификат корневого центра сертификации;

заархивировать (обязательно!) сертификат и скриншот;

отправить архив на адрес электронной почты <u>0990@minfin.ru</u> с указанием, наименования учреждения, ФИО пользователя, логина в Системе и действий, которые привели к ошибке.

При возникновении вопросов, связанных с функционированием Системы необходимо обращаться по телефону: 8 800 333-62-26 или по электронной почте support.budgetplan@minfin.ru.