МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПИСЬМО
от 17 июня 2016 г. N 21-03-04/35490

В соответствии с пунктом 4 Правил формирования, утверждения и ведения плана закупок товаров, работ, услуг для обеспечения федеральных нужд, а также требований к форме плана закупок товаров, работ, услуг для обеспечения федеральных нужд, утвержденных постановлением Правительства Российской Федерации от 05.06.2015 N 552, государственные заказчики, действующие от имени Российской Федерации, должны до 1 июля текущего года сформировать и представить главным распорядителям средств федерального бюджета (далее - главным распорядителям бюджетных средств) планы закупок в целях формирования на их основании в соответствии с бюджетным законодательством Российской Федерации обоснований бюджетных ассигнований на осуществление закупок.

В соответствии с частью 1 статьи 4 Федерального закона от 05.06.2013 N 44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" и подпункта "б" пункта 35 Положения о государственной интегрированной информационной системе управления общественными финансами "Электронный бюджет" (далее - система "Электронный бюджет"), утвержденного постановлением Правительства Российской Федерации от 30.06.2015 N 658, в подсистеме управления закупками системы "Электронный бюджет" обеспечена возможность формирования планов закупок для представления их главным распорядителям бюджетных средств.

В целях обеспечения доступа к подсистеме управления закупками системы "Электронный бюджет" необходимо выполнить подготовительные мероприятия и предоставить в орган Федерального казначейства по месту обслуживания главных распорядителей бюджетных средств и подведомственных им государственных заказчиков, действующих от имени Российской Федерации соответственно, заявки на подключение к подсистеме управления закупками системы "Электронный бюджет", содержащие информацию о сотрудниках:

государственных заказчиков, действующих от имени Российской Федерации, ответственных за формирование планов закупок (по форме согласно приложениям 1 - 3 к настоящему письму);

главных распорядителей бюджетных средств, ответственных за рассмотрение представленных планов закупок (по форме согласно приложениям 4 - 6 к настоящему письму).

При необходимости разграничения доступа сотрудников государственных заказчиков к формируемой информации необходимо заполнить в заявке графу "Ограничение на полномочие", указав для отдельных сотрудников коды видов расходов "200", "300" и/или "400", в

соответствии с которыми ими может осуществляться формирование (согласование) отдельных закупок, включаемых в план закупок.

Временный порядок подключения к подсистеме управления закупками системы "Электронный бюджет", приведен в приложении 7 к настоящему письму.

В целях организации обучения работе в подсистеме управления закупками системы "Электронный бюджет", прошу в срок до 24 июня 2016 года направить в Федеральное казначейство информацию о готовности главных распорядителей бюджетных средств и подведомственных им государственных заказчиков, действующих от имени Российской Федерации начать работу по формированию планов закупок в подсистеме управления закупками системы "Электронный бюджет".

При возникновении вопросов, связанных с организацией доступа к подсистеме управления закупками системы "Электронный бюджет" и получения СКЗИ, необходимо обращаться к сотрудникам органа Федерального казначейства по месту обслуживания.

Т.Г.НЕСТЕРЕНКО

Приложение 1
к письму Министерства финансов
Российской Федерации
от 17 июня 2016 г. N 21-03-04/35490

ЗАЯВКА
на подключение к подсистеме управления закупками
государственной интегрированной информационной системы
управления общественными финансами "Электронный бюджет"
уполномоченных лиц государственных заказчиков, действующих
от имени Российской Федерации

Наименование главного распорядителя средств федерального бюджета	
Код организации в соответствии с реестром участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса	
Наименование государственного заказчика, действующего от имени Российской Федерации	
Код организации в соответствии с реестром участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса	
Подразделение	

Должность			
ФИО			
СНИЛС			
Контактный телефон	+7 (___) ___ - __ - __	+ доб. номер	
Адрес электронной почты			
Информация о сертификате (серийный номер сертификата пользователя или наименование файла, содержащего сертификат)			

Полномочия			
<Наименование полномочия>			
Ввод данных	Согласование	Утверждение	Просмотр

Добавить	Добавить	Добавить	Добавить
Ограничения на полномочие <1>			

```
Сотрудник государственного
заказчика, действующего
от имени Российской Федерации
(пользователь)                _____________          _____________________________
                                (подпись)              (расшифровка подписи)

Руководитель государственного
заказчика, действующего
от имени Российской Федерации
/Уполномоченное лицо
государственного заказчика,
действующего от имени
Российской Федерации          _____________          _____________________________
                                (подпись)              (расшифровка подписи)
                        М.П.
```

<1> Указываются при необходимости разграничения доступа. При отсутствии необходимости в разграничении доступа данное поле не заполняется.

Приложение 2

к письму Министерства финансов
Российской Федерации
от 17 июня 2016 г. N 21-03-04/35490

ЗАЯВКА
на изменение сведений и полномочий уполномоченных лиц государственных заказчиков, действующих от имени Российской Федерации в подсистеме управления закупками государственной интегрированной информационной системы управления общественными финансами "Электронный бюджет"

Наименование главного распорядителя средств федерального бюджета	
Код организации в соответствии с реестром участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса	
Наименование государственного заказчика, действующего от имени Российской Федерации	
Код организации в соответствии с реестром участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса	

Подразделение			
Должность			
ФИО			
СНИЛС			
Контактный телефон	+7 (___) ___ - __ - __	+ доб. номер	
Адрес электронной почты			
Информация о сертификате (серийный номер сертификата пользователя или наименование файла, содержащего сертификат)			

Полномочия
<Наименование полномочия>

Ввод данных	Согласование	Утверждение	Просмотр
Добавить/Исключить	Добавить/Исключить	Добавить/Исключить	Добавить/Исключить
Ограничения на полномочие <1>			

Сотрудник государственного
заказчика, действующего
от имени Российской Федерации
(пользователь) _____ _____
(подпись) (расшифровка подписи)

Руководитель государственного
заказчика, действующего
от имени Российской Федерации
/Уполномоченное лицо
государственного заказчика,
действующего от имени
Российской Федерации _____ _____
(подпись) (расшифровка подписи)
М.П.

<1> Указываются при необходимости разграничения доступа указываются. При отсутствии необходимости в разграничении доступа данное поле не заполняется.

Приложение 3
к письму Министерства финансов
Российской Федерации
от 17 июня 2016 г. N 21-03-04/35490

ПЕРЕЧЕНЬ ПОЛНОМОЧИЙ
в подсистеме управления закупками государственной интегрированной информационной системы управления общественными финансами "Электронный бюджет" уполномоченных лиц государственных заказчиков, действующих от имени Российской Федерации

Полномочия сотрудников			
Планирование закупок			
Ввод данных	Согласование	Утверждение	Просмотр

Ограничения на полномочие
Планирование закупок
1. Указываются коды видов расходов по бюджетной классификации Российской Федерации, в соответствии, с которыми осуществляется формирование предложений по закупкам (например: 200, 300, 400)
2. Указываются наименование документов, формируемых в рамках полномочия (например: предложение по закупкам, план закупок)

Приложение 4
к письму Министерства финансов
Российской Федерации
от 17 июня 2016 г. N 21-03-04/35490

ЗАЯВКА
на подключение к подсистеме управления закупками
государственной интегрированной информационной системы
управления общественными финансами "Электронный бюджет"
уполномоченных лиц главных распорядителей средств
федерального бюджета

Наименование главного распорядителя средств федерального бюджета	
Код организации в соответствии с реестром участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса	
Подразделение	

Должность			
ФИО			
СНИЛС			
Контактный телефон	+7 (___) ___ - __ - __	+ доб. номер	
Адрес электронной почты			
Информация о сертификате (серийный номер сертификата пользователя или наименование файла, содержащего сертификат)			

Полномочия			
<Наименование полномочия>			
Ввод данных	Согласование	Утверждение	Просмотр

Добавить	Добавить	Добавить	Добавить
Ограничение на полномочие <1>			

Сотрудник главного
распорядителя средств
федерального бюджета
(пользователь) _____ _____
(подпись) (расшифровка подписи)

Руководитель главного
распорядителя средств
федерального бюджета
/Уполномоченное лицо
главного распорядителя средств
федерального бюджета _____ _____
(подпись) (расшифровка подписи)
М.П.

<1> Указываются при необходимости разграничения доступа указываются. При отсутствии необходимости в разграничении доступа данное поле не заполняется.

Приложение 5
к письму Министерства финансов
Российской Федерации
от 17 июня 2016 г. N 21-03-04/35490

ЗАЯВКА
на изменение сведений и полномочий уполномоченных лиц
главных распорядителей средств федерального бюджета
в подсистеме управления закупками государственной
интегрированной информационной системы управления
общественными финансами "Электронный бюджет"

Наименование главного распорядителя средств федерального бюджета	
Код организации в соответствии с реестром участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса	
Подразделение	
Должность	
ФИО	
СНИЛС	

Контактный телефон	+7 (___) ___ - __ - __	+ доб. номер	
Адрес электронной почты			
Информация о сертификате (серийный номер сертификата пользователя или наименование файла, содержащего сертификат)			

Полномочия			
<Наименование полномочия>			
Ввод данных	Согласование	Утверждение	Просмотр
Добавить/Исключить	Добавить/Исключить	Добавить/Исключить	Добавить/Исключить
Ограничение на полномочие <1>			

Сотрудник главного
распорядителя средств
федерального бюджета
(пользователь) _____ _____
(подпись) (расшифровка подписи)

Руководитель главного
распорядителя средств
федерального бюджета
/Уполномоченное лицо
главного распорядителя средств
федерального бюджета _____ _____
М.П.

<1> Указываются при необходимости разграничения доступа. При отсутствии необходимости в разграничении доступа данное поле не заполняется.

Приложение 6
к письму Министерства финансов
Российской Федерации
от 17 июня 2016 г. N 21-03-04/35490

ПЕРЕЧЕНЬ ПОЛНОМОЧИЙ
в подсистеме управления закупками государственной
интегрированной информационной системы управления
общественными финансами "Электронный бюджет" уполномоченных
лиц главных распорядителей средств федерального бюджета

Полномочия сотрудников главных распорядителей средств федерального бюджета

Планирование закупок			
			Просмотр

Ограничения на полномочие
Планирование закупок
1. Указываются наименование документов, формируемых в рамках полномочия (например: план закупок)

Приложение N 7
к письму Министерства финансов
Российской Федерации
от 17 июня 2016 г. N 21-03-04/35490

ВРЕМЕННЫЙ ПОРЯДОК ПОДКЛЮЧЕНИЯ К ПОДСИСТЕМЕ УПРАВЛЕНИЯ ЗАКУПКАМИ СИСТЕМЫ "ЭЛЕКТРОННЫЙ БЮДЖЕТ"

I. Перечень мероприятий, которые необходимо выполнить для подключения к подсистеме управления закупками системы "Электронный бюджет"

1. Подготовка информационно-технологической инфраструктуры к подключению к подсистеме управления закупками системы "Электронный бюджет"

Для подготовки информационно-технологической инфраструктуры к подключению должны быть выполнены следующие мероприятия:

а) определен ответственный за техническое обеспечение работы и подключение сотрудников;

б) получены специальные средства криптографической защиты информации, обеспечивающие создание защищенного соединения с подсистемой управления закупками системы "Электронный бюджет" (далее - СКЗИ), лицензионные ключи и эксплуатационную документацию к СКЗИ в органе Федерального казначейства;

в) обеспечено соответствие автоматизированных рабочих мест пользователей требованиям к автоматизированному рабочему месту, с которого осуществляется доступ к подсистеме управления закупками системы "Электронный бюджет" (приложение N 1 к настоящему Порядку), включая установку и настройку СКЗИ на автоматизированных рабочих местах пользователей;

г) выполнены требования по обеспечению информационной безопасности автоматизированного рабочего места, с которого осуществляется доступ к подсистеме управления закупками системы "Электронный бюджет" (приложение N 2 к настоящему Порядку).

Для получения СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ необходимо:

оформить доверенность на получение СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ ответственному за техническое обеспечение работы и подключение сотрудников (по форме, согласно приложению 3 к настоящему Порядку);

направить в орган Федерального казначейства заявку о выдаче СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ (по форме, согласно приложению 4 к настоящему Порядку). Заявка о выдаче СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ может быть представлена одновременно с заявкой на подключение к подсистеме управления закупками системы "Электронный бюджет".

2. Мероприятия по подключению сотрудников организаций к подсистеме управления закупками системы "Электронный бюджет"

Для подключения сотрудников к подсистеме управления закупками системы "Электронный бюджет" необходимо провести следующие мероприятия:

а) определить сотрудников:

государственных заказчиков, действующих от имени Российской Федерации, ответственных за формирование планов закупок;

главных распорядителей средств федерального бюджета, ответственных за рассмотрение планов закупок.

б) обеспечить наличие у сотрудников квалифицированных сертификатов ключей проверки электронных подписей (далее - сертификатов);

в) представить в органы Федерального казначейства по месту нахождения организации заявки на подключение, указанные в письме, подписанные руководителем или иным уполномоченным лицом организации, на бумажном носителе в двух экземплярах (заявки представляются ответственным за техническое обеспечение работы и подключение сотрудников).

Одновременно с заявками на подключение в орган Федерального казначейства предоставляются:

документ, подписанный руководителем, определяющий ответственного за техническое обеспечение работы и подключение сотрудников (если ранее не предоставлялся);

заверенная в установленном порядке копия распорядительного документа или доверенность, подтверждающие право уполномоченного лица действовать от имени организации, в случае если заявка на подключение подписана не руководителем организации, а иным уполномоченным лицом организации;

файл действующего сертификата каждого подключаемого сотрудника (на съемном носителе информации);

согласие на обработку персональных данных каждого подключаемого сотрудника (приложение N 5 к настоящему Порядку).

3. Мероприятия, проводимые органом Федерального казначейства, при рассмотрении заявки на подключение к подсистеме управления закупками системы "Электронный бюджет"

Орган Федерального казначейства в течение 3 (трех) рабочих дней со дня предоставления заявки на подключение к подсистеме управления закупками системы "Электронный бюджет" осуществляет проверку ее содержания на:

соответствие заявки на подключение установленной форме;

наличие действующего на момент рассмотрения заявки на подключение сертификата сотрудника, включенного в Заявку на подключение;

идентичность сведений о сотруднике, указанных в заявке на подключение, соответствующим сведениям в предоставленном сертификате;

наличие документов, указанных в разделе 2 настоящего Порядка.

По результатам проверки заявки на подключение и сертификата орган Федерального казначейства формирует информацию о результатах проверки отдельно по каждому пользователю, указанному в заявке на подключение.

В случае положительного результата проверки заявки на подключение орган Федерального казначейства на основании сведений, содержащихся в заявке на подключение, предоставляет сотрудникам организации доступ к подсистеме управления закупками системы "Электронный бюджет".

Не позднее 2 (двух) рабочих дней со дня предоставления доступа сотруднику к подсистеме управления закупками системы "Электронный бюджет" орган Федерального казначейства уведомляет ответственного за техническое обеспечение работы и подключение пользователей о предоставлении доступа к компонентам системы "Электронный бюджет" посредством направления на бумажном носителе извещения Федерального казначейства о результатах отработки заявки на подключение (приложение N 6 к настоящему Порядку).

В случае отрицательного результата проверки заявки на подключение доступ сотруднику к подсистеме управления закупками системы "Электронный бюджет" не предоставляется и орган Федерального казначейства не позднее 2 (двух) рабочих дней после проверки заявки на подключение уведомляет ответственного за техническое обеспечение работы и подключение сотрудников об отказе в предоставлении доступа к подсистеме управления закупками системы "Электронный бюджет" с указанием выявленных несоответствий и (или) основания, по которым доступ не предоставлен, посредством направления на бумажном носителе извещения Федерального казначейства о результатах отработки заявки на подключение.

Приложение N 1
к Порядку подключения к подсистеме
управления закупками системы
"Электронный бюджет"

ТРЕБОВАНИЯ К АВТОМАТИЗИРОВАННОМУ РАБОЧЕМУ МЕСТУ, С КОТОРОГО ОСУЩЕСТВЛЯЕТСЯ ДОСТУП К ПОДСИСТЕМЕ УПРАВЛЕНИЯ ЗАКУПКАМИ СИСТЕМЫ "ЭЛЕКТРОННЫЙ БЮДЖЕТ"

В целях подключения к подсистеме управления закупками системы "Электронный бюджет" автоматизированное рабочее место (далее - АРМ) должно соответствовать следующим техническим требованиям:

1. Минимальные аппаратные характеристики АРМ приведены в таблице 1.

Таблица 1. Минимальные аппаратные характеристики АРМ

Параметр (не менее)	Значение
Процессор, Ггерц	2.0
Объем ОЗУ, Мбайт	1024
Объем свободного места на жестком диске, Мбайт	500
Порт USB 2.0 или 3.0	1

2. Перечень операционных систем, которые могут быть установлены на АРМ:

- Microsoft Windows XP;
- Microsoft Windows Vista;
- Microsoft Windows 7;
- Microsoft Windows 8;
- Microsoft Windows 8.1;
- Microsoft Windows 2003 Server SP2;
- Microsoft Windows 2003 Server R2 SP2;
- Microsoft Windows 2008 Server SP2;
- Microsoft Windows 2008 Server R2 SP1.

Поддерживается как 32-битная, так и 64-битная архитектуры операционных систем.

Допускается применение любого официального пакета обновлений операционных систем.

3. Перечень веб-обозревателей и их версий, которые могут быть использованы для обеспечения входа в личный кабинет сотрудника:

- Internet Explorer версии 10.0 или выше;
- Mozilla Firefox версии 32.0 или выше;
- Google Chrome версии 38.0 или выше;
- Opera версии 25.0 или выше.

4. Перечень обязательного к установке программного обеспечения:

- ПО "Windows Installer";
- Драйвер используемого носителя ключевой информации сертификата пользователя;
- Средство создания защищенного TLS-соединения "Континент TLS Клиент";
- Средство электронной подписи "Jinn-Client".

При работе с подсистемой управления закупками системы "Электронный бюджет" могут быть использованы следующие носители ключевой информации сертификата пользователя:

- USB флеш-накопитель;
- Rutoken S;
- eToken Pro;
- eToken PRO (Java).

Приложение N 2
к Порядку подключения к подсистеме
управления закупками системы
"Электронный бюджет"

ТРЕБОВАНИЯ
ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННОГО РАБОЧЕГО МЕСТА, С КОТОРОГО ОСУЩЕСТВЛЯЕТСЯ ДОСТУП К ПОДСИСТЕМЕ УПРАВЛЕНИЯ ЗАКУПКАМИ СИСТЕМЫ "ЭЛЕКТРОННЫЙ БЮДЖЕТ"

1. В настоящем приложении используются следующие термины и сокращения:

АО - аппаратное обеспечение;

АРМ - автоматизированное рабочее место сотрудника;

ВВК - воздействие вредоносного кода;

ВК - вредоносный код;

ЛВС - локальная вычислительная сеть;

НСД - несанкционированный доступ;

ОС - операционная система;

ПО - программное обеспечение;

ПАК - программного-аппаратный комплекс;

СЗИ - средства защиты информации;

СКЗИ - специальные средства криптографической защиты информации.

2. В целях защиты ПО и АО от НСД и ВВК необходимо:

- обеспечить применение СЗИ от НСД и ВВК;

- реализовать комплекс организационно-технических и административных мероприятий, связанных с обеспечением правильности функционирования технических средств обработки и передачи информации;

- установить соответствующие правила для обслуживающего персонала, допущенного к работе с информацией ограниченного доступа.

3. Защита информации от НСД должна обеспечиваться на всех технологических этапах обработки информации, в том числе при проведении ремонтных и регламентных работ. Защита информации от НСД должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем или администратором информационной безопасности. В организации, эксплуатирующей АРМ, должен быть назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по использованию АРМ, выработки соответствующих инструкций для сотрудников, а также контроль за соблюдением описанных ниже требований.

4. При размещении технических средств с установленным АРМ:

должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным АРМ, посторонних лиц, по роду своей деятельности не являющихся персоналом, допущенным к работе в этих помещениях;

внутренняя планировка, расположение и укомплектованность рабочих мест в помещениях должны обеспечивать сотрудникам сохранность

доверенных им конфиденциальных документов и сведений, включая ключевую информацию.

5. К установке общесистемного и специального ПО допускаются лица, изучившие документацию на ПО. При установке ПО на АРМ необходимо соблюдать следующие требования:

1) на технических средствах, предназначенных для работы с АРМ, использовать только лицензионное ПО фирм-изготовителей;

2) установку ПО АРМ необходимо производить только с зарегистрированного, защищенного от записи носителя;

3) на АРМ не должны устанавливаться средства разработки ПО и отладчики;

4) предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств, на которых установлено ПО АРМ (например, путем опечатывания системного блока и разъемов АРМ);

5) после завершения процесса установки должны быть выполнены действия, необходимые для осуществления периодического контроля целостности установленного ПО на АРМ;

6) ПО, устанавливаемое на АРМ, не должно содержать возможностей, позволяющих:

- модифицировать содержимое произвольных областей памяти;
- модифицировать собственный код и код других подпрограмм;
- модифицировать память, выделенную для других подпрограмм;
- передавать управление в область собственных данных и данных других подпрограмм;
- не санкционированно модифицировать файлы, содержащие исполняемые коды при их хранении на жестком диске;
- повышать предоставленные привилегии;
- модифицировать настройки ОС;
- использовать недокументированные фирмой-разработчиком функции ОС.

6. При организации работ по защите информации от НСД необходимо учитывать следующие требования:

1) необходимо разработать и применить политику назначения и смены паролей (для входа в ОС, BIOS, при шифровании на пароле и т.д.), использовать фильтры паролей в соответствии со следующими правилами:

- длина пароля должна быть не менее 8-ми символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #,$,&,*, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (USER, ADMIN, ALEX и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в 4-х позициях;

- личный пароль пользователь не имеет права сообщать никому;

- периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 6-и месяцев. Число неудачных попыток ввода пароля должно быть ограничено числом 10.

Указанная политика обязательна для всех учетных записей, зарегистрированных в ОС;

2) средствами BIOS должна быть исключена возможность работы на АРМ, если во время его начальной загрузки не проходят встроенные тесты;

3) запрещается:

- оставлять без контроля вычислительные средства, на которых эксплуатируется АРМ, после ввода ключевой информации либо иной информации ограниченного доступа;

- осуществлять несанкционированное администратором информационной безопасности копирование ключевых носителей;

- разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей, принтер и т.п. иные средства отображения информации;

- записывать на ключевые носители постороннюю информацию.

4) администратор информационной безопасности должен сконфигурировать ОС, в среде которой планируется использовать АРМ, и осуществлять периодический контроль сделанных настроек в соответствии со следующими требованиями:

- не использовать нестандартные, измененные или отладочные версии ОС;

- исключить возможность загрузки и использования ОС, отличной от предусмотренной штатной работой;

- исключить возможность удаленного управления, администрирования и модификации ОС и ее настроек;

- режимы безопасности, реализованные в ОС, должны быть настроены на максимальный уровень;

- всем сотрудникам и группам, зарегистрированным в ОС, необходимо назначить необходимые для нормальной работы права доступа;

- должно быть исключено попадание в систему программ, позволяющих, пользуясь ошибками ОС, повышать предоставленные привилегии;

- необходимо регулярно устанавливать пакеты обновления безопасности ОС (Service Packs, Hot fix и т.п.), обновлять антивирусные базы, а также исследовать информационные ресурсы по вопросам компьютерной безопасности с целью своевременной минимизации опасных последствий от возможного воздействия на ОС;

- необходимо организовать и использовать систему аудита, организовать регулярный анализ результатов аудита;

- необходимо организовать и использовать комплекс мероприятий антивирусной защиты;

- необходимо исключить одновременную работу ОС с загруженной ключевой информацией нескольких сотрудников.

7. Для работы АРМ с подсистемой управления закупками требуется применять программно-аппаратные СЗИ от НСД не ниже 6 класса защищенности для СВТ, такие как "Secret Net", "Соболь", "Панцирь-С" и т.п.

8. При наличии технической возможности, обновление средств защиты и сигнатурных баз производится централизованно, с рабочего места администратора программных средств защиты от воздействий вредоносного кода. При проведении централизованных обновлений используется механизм ведения протокола средств защиты. Обновление сигнатурных баз производится по мере их выпуска.

В целях обеспечения защиты от воздействий вредоносного кода пользователю АРМ запрещается:

- самостоятельно устанавливать программное обеспечение, в том числе командные файлы;

- использовать при работе "зараженный" вредоносным кодом либо с подозрением на "заражение" носитель и/или файл;

- использовать личные носители на АРМ;

- использовать служебные носители на домашних компьютерах и в неслужебных целях;

- самостоятельно проводить "лечение" носителя и/или файла;

- самостоятельно отключать, удалять и изменять настройки установленных средств защиты.

Сотрудник, которому установлен АРМ обязан:

- проводить контроль на отсутствие ВК любых сменных и подключаемых носителей (CD-дисков, DVD-дисков, USB флеш-накопителей и т.п.) и файлов, за исключением ключевых носителей средств криптографической защиты информации;

- на компьютерах с отключенным антивирусным монитором (постоянной защитой) проводить полную проверку на отсутствие ВК еженедельно (в первый день после выходных);

- при появлении сообщений, формируемых средствами защиты информации, об обнаружении вредоносного кода немедленно прекратить работу и сообщить об этом руководителю и администратору информационной безопасности (или сотруднику, выполняющему эти функции);

- при невозможности запуска средств защиты информации или при ошибках в процессе их выполнения немедленно прекратить работу и сообщить об этом руководителю и администратору информационной безопасности (или сотруднику, выполняющему эти функции).

Правила и рекомендации сотруднику по защите от воздействий вредоносного кода:

- первичный входной контроль на отсутствие ВК носителей, предназначенных для многоразовой записи информации (перезаписываемых компакт-дисков и DVD-дисков, USB флеш-накопителей и других подобных

носителей) проводится при первом применении носителя на данном компьютере. Последующие контроли носителя производятся перед каждым просмотром состава и содержимого файлов;

- в целях исключения автозапуска исполняемых файлов со сменных носителей (CD, DVD, USB флеш-накопителей и т.п.) рекомендуется при присоединении носителя к компьютеру (вставка CD/DVD в лоток, вставка USB флеш-накопителей в порт USB) удерживать некоторое время (20 - 30 секунд) нажатой клавишу Shift;

- входной контроль на отсутствие ВК компакт-дисков и DVD-дисков, предназначенных для одноразовой записи информации, проводит получатель (владелец) диска однократно с момента приобретения (получения) диска перед использованием его на компьютерах.

9. Для работы АРМ с подсистемой управления закупками требуется применять программные средства защиты от воздействия вредоносного кода не ниже 5 класса защищенности по типу Г, таких как: "Kaspersky Endpoint Security для Windows", "Security Studio Endpoint", "OfficeScan" и т.п.

10. Состав СЗИ, применяемых на АРМ, зависит от способа взаимодействия АРМ пользователя с подсистемой управления закупками. По способу взаимодействия с подсистемой управления закупками АРМ подразделяется на следующие типы:

- Тип 1 - АРМ, взаимодействующий с подсистемой управления закупками посредством прямого подключения к сети Интернет.

- Тип 2 - АРМ, взаимодействующий с подсистемой управления закупками посредством подключения к сети Интернет через ЛВС организации.

- Тип 3 - АРМ, взаимодействующий с подсистемой управления закупками посредством подключения по выделенным каналам связи через ЛВС организации.

11. Взаимодействие АРМ Тип 1 должно быть защищено с помощью:

- персонального средства межсетевого экранирования не ниже 4 класса защищенности, таких как: "Континент-АП", "Security Studio Endpoint Protection", "ViPNet Client" и т.п.;

- персонального средства обнаружения вторжений не ниже 6 класса защищенности для СВТ.

В качестве средства обнаружения вторжений может быть использовано ПО "Security Studio Endpoint Protection" либо иное средство, сертифицированное по требуемому классу защищенности.

12. Взаимодействие АРМ Тип 2 и Тип 3 должно быть защищено с помощью:

- сетевого (в составе ЛВС Организации) или персонального средства межсетевого экранирования не ниже 4 класса защищенности.

Примеры допустимых к использованию по классу защищенности средств межсетевого экранирования:

1) в составе ЛВС организации:

- АПКШ Континент;

- Check Point Firewall;
- ViPNet Coordinator и т.п.

2) персональные средства:

- Security Studio Endpoint Protection;
- Континент-АП;
- ViPNet Client (4 класс) и т.п.

- сетевого (в составе ЛВС организации) или персонального средства обнаружения вторжений не ниже 5 класса защищенности.

Примеры допустимых к использованию по классу защищенности средств обнаружения вторжений:

1) персональные средства или средства в составе ЛВС организации:

- Континент-ДА;
- Security Studio Endpoint Protection и т.п.

13. Установка, настройка и сопровождение СКЗИ осуществляется администратором информационной безопасности организации в соответствии с требованиями законодательства Российской Федерации и эксплуатационной документации к СКЗИ.

Первичная установка СКЗИ на АРМ осуществляется с оформлением акта установки.

Формуляр на СКЗИ в электронном виде, находящийся в составе документации на СКЗИ, выводится администратором информационной безопасности организации на бумажный носитель и заполняется от руки в части раздела "Сведения о закреплении изделия при эксплуатации". Ответственное хранение формуляра осуществляется администратором информационной безопасности организации.

Запрещается полное или частичное воспроизведение, тиражирование и распространение оптических носителей, содержащих дистрибутивы СКЗИ, а также лицензионных ключей СКЗИ.

В случае прекращения доступа организации к подсистеме управления закупками, оптические носители, содержащие дистрибутивы СКЗИ, и лицензионные ключи СКЗИ, а также заполненные установленным порядком формуляры возвращаются организацией в орган Федерального казначейства (по месту получения СКЗИ).

Приложение N 3
к Порядку подключения к подсистеме
управления закупками системы
"Электронный бюджет"

Примерная форма <1>

Доверенность N ____

"__" _____ 20__ г.

_____
(наименование организации)
в лице _____
(фамилия, имя, отчество руководителя)
действующего на основании _____
уполномочивает _____
(фамилия, имя, отчество)
_____
(серия и номер паспорта, кем и когда выдан)

предоставлять в Федеральное казначейство заявительные документы в целях получения средств криптографической защиты информации (далее - СКЗИ), лицензионных ключей и эксплуатационной документации к СКЗИ, необходимых для обеспечения создания защищенного соединения с компонентами системы "Электронный бюджет".

Получать СКЗИ, лицензионные ключи и эксплуатационную документацию к данным средствам в соответствии с предоставленными заявительными документами.

Представитель наделяется правом подписи документов на получение СКЗИ, лицензионных ключей и эксплуатационной документации к данным средствам в соответствии с предоставленными заявительными документами.

Настоящая доверенность действительна по "__" _____ 20__ г.

Подпись руководителя организации _____/_____/
(подпись) (расшифровка подписи)

Подпись уполномоченного лица _____/_____/
(подпись) (расшифровка подписи)

Оформляется на бланке письма организации

Приложение N 4
к Порядку подключения к подсистеме
управления закупками системы
"Электронный бюджет"

ЗАЯВКА
на выдачу СКЗИ, лицензионных ключей
и эксплуатационной документации к СКЗИ

(наименование органа
Федерального казначейства)

от "__" _____ 20__ г. N _____

Для целей обеспечения создания защищенного соединения с компонентами системы "Электронный бюджет" и обеспечения работы с усиленной квалифицированной электронной подписью просим выдать средства криптографической защиты информации, лицензионные ключи в количестве _____

штук и эксплуатационную документацию к данным средствам.

(должность руководителя
организации или иного
уполномоченного лица) _____ _____
(подпись) (инициалы, фамилия)

Приложение N 5
к Порядку подключения к подсистеме
управления закупками системы
"Электронный бюджет"

ОБРАЗЕЦ СОГЛАСИЯ НА ОБРАБОТКУ ПЕРСОНАЛЬНЫХ ДАННЫХ

СОГЛАСИЕ
на обработку персональных данных

Я, _____,
фамилия, имя, отчество
проживающий по адресу (по месту регистрации) _____
_____
_____ паспорт _____ N _____ дата выдачи _____ название выдавшего органа _____, в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", даю свое согласие _____
_____
(указывается наименование органа Федерального казначейства,
которому дается согласие)
на автоматизированную, а также без использования средств автоматизации, обработку моих персональных данных, включающих фамилию, имя, отчество, должность, сведения о месте работы, адрес электронной почты, контактный(е) телефон(ы), страховой номер индивидуального лицевого счета в Пенсионном фонде России (СНИЛС), в целях осуществления действий по подключению к компонентам государственной интегрированной системы управления общественными финансами "Электронный бюджет". Предоставляю указанному органу Федерального казначейства право осуществлять все действия (операции) с моими персональными данными, включая сбор, систематизацию, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение.

Срок действия настоящего согласия - период времени до истечения установленных нормативными актами сроков хранения соответствующей информации или документов, размещенных в компонентах системы "Электронный бюджет" с использованием моей электронной подписи.

Настоящее согласие на обработку персональных данных может быть отозвано в порядке, установленном Федеральным законом Российской Федерации от 27.07.2006 N 152-ФЗ "О персональных данных". В случае отзыва согласия на обработку моих персональных данных указанный орган Федерального казначейства вправе не прекращать их обработку до окончания срока действия настоящего согласия.

Контактный(е) телефон(ы) _____

Подпись субъекта персональных данных _____ _____
подпись Ф.И.О.

"__" _____ 20__ г.

Приложение N 6
к Порядку подключения к подсистеме
управления закупками системы
"Электронный бюджет"

Извещение
Федерального казначейства о результатах отработки Заявки
на подключение к компонентам системы "Электронный бюджет"
от "__" _____ 20__ г.

Результат отработки:

Наименование организации _____

Заявка ФИО _____
Заявка ФИО _____
_____
<доступ предоставлен/не предоставлен/прекращен,
полномочия изменены/не изменены>

Примечания _____
<указывается причина в случае отказа>

Ответственный исполнитель	---	---	---	---
	(должность)	(подпись)	(расшифровка подписи)	(телефон)

" " _____ 20__ г.

Извещение получил	---	---	---	---
	(должность)	(подпись)	(расшифровка подписи)	(телефон)

" " _____ 20__ г.

<1> Оформляется на бланке письма организации.