МИНИСТЕРСТВО ФИНАНСОВ
РОССИЙСКОЙ ФЕДЕРАЦИИ
(МИНФИН РОССИИ)

ПЕРВЫЙ
ЗАМЕСТИТЕЛЬ МИНИСТРА

Ильинка, д. 9, Москва, 109097
телетайп: 112008
телефакс: +7 (495) 625-08-89

18.05.2015 № 21-10-07/28192

На № _____

Главные распорядители средств федерального бюджета, органы управления государственными внебюджетными фондами, Центральный банк Российской Федерации
(согласно списку рассылки)

В рамках реализации приказа Министерства финансов Российской Федерации от 23 декабря 2014 г. № 163н «О порядке формирования и ведения реестра участников бюджетного процесса, а также юридических лиц, не являющихся участниками бюджетного процесса» представление информации и документов в целях формирования и ведения реестра участников бюджетного процесса юридических лиц, не являющихся участниками бюджетного процесса (далее – ведение реестра участников бюджетного процесса) будет осуществляться в государственной интегрированной информационной системы управления общественными финансами «Электронной бюджет» (далее – компоненты системы «Электронный бюджет»).

В целях организации работ по предоставлению доступа к компонентам системы «Электронный бюджет» сотрудников главных распорядителей средств федерального бюджета, органов управления государственными внебюджетными фондами и Центрального банка Российской Федерации (далее – Уполномоченные организации) и организации обучения работе в информационной системе, прошу в срок до 25 мая 2015 года предоставить в Межрегиональное операционное управление Федерального казначейства заявки на предоставление доступа к компонентам системы «Электронный бюджет», содержащие, в том числе, информацию о сотрудниках, ответственных за ведение реестра участников бюджетного процесса (по форме согласно приложению 1 к настоящему письму).

Доступ к компонентам системы «Электронный бюджет» разграничивается в зависимости от полномочий по вводу, согласованию, утверждению и просмотру данных, а также координации пользователей.

1) Для подключения к компонентам системы «Электронный бюджет» и обеспечения использования электронной подписи используются специальные

средства криптографической защиты информации, обеспечивающие создание защищенного соединения с компонентами системы «Электронный бюджет» и средства электронной подписи (далее – СКЗИ). СКЗИ будут предоставлены Межрегиональным операционным управлением Федерального казначейства Уполномоченной организации в соответствии с заявкой о выдаче СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ (по форме согласно приложению 2 к настоящему письму).

Получение СКЗИ на Уполномоченную организацию и всех пользователей Уполномоченной организации осуществляется ответственным за техническое обеспечение работы с компонентами системы «Электронный бюджет» и подключение пользователей, действующим по доверенности (по форме согласно приложению 3 к настоящему письму) в течение 5 рабочих дней после предоставления в Межрегиональное операционное управление Федеральное казначейство заявки о выдаче СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ.

2) Для обеспечения юридически значимого электронного документооборота в компонентах системы «Электронный бюджет» используется усиленная квалифицированная электронная подпись. Квалифицированные сертификаты ключей проверки электронных подписей (далее – сертификат) должны быть выданы удостоверяющим центром, получившим аккредитацию на соответствие установленным законодательством Российской Федерации требованиям.

В случае необходимости, сертификаты могут быть выданы органом Федерального казначейства в соответствии с Регламентом Удостоверяющего центра Федерального казначейства, размещенным на официальном сайте Федерального казначейства в разделе «Удостоверяющий центр/Нормативные документы».

Подробный перечень мероприятий, которые необходимо выполнить для подключения к компонентам системы «Электронный бюджет» приведен в приложении 4 к настоящему письму.

При возникновении вопросов, связанных с организацией доступа к информационной системе Минфина России и получения СКЗИ, необходимо обращаться к сотрудникам Межрегионального операционного управления Федерального казначейства по телефонам:

8 (495) 915-57-82,

8 (495) 698-05-73.

Приложение:

1. Форма заявки на подключение к компонентам системы «Электронный

бюджет» для ведения реестра участников бюджетного процесса на 2 л. в 1 экз.;

2. Форма заявки о выдаче СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ на 1 л. в 1 экз.;

3. Примерная форма доверенности на 1 л. в 1 экз.;

4. Перечень мероприятий, которые необходимо выполнить Уполномоченной организации для подключения к компонентам системы «Электронный бюджет» на __ л. в 1 экз.

Т.Г. Нестеренко

Приложение № 1
к письму Министерства финансов
Российской Федерации
от «___»_____2015 г. № _____

Форма заявки на подключение к компонентам системы «Электронный бюджет» для ведения реестра участников бюджетного процесса

_____
(указывается наименование органа Федерального казначейства)

ЗАЯВКА
на подключение к компонентам системы «Электронный бюджет»
для ведения реестра участников бюджетного процесса

от «___» _____ 20__ г.

Наименование организации	_____	ОГРН
		ИНН
Юридический адрес	_____	КПП
Контактный телефон организации	_____	
Адрес электронной почты организации	_____	

Прошу осуществить подключение организации и/или регистрацию (изменение) данных об указанных пользователях к компонентам системы «Электронный бюджет» **для ведения реестра участников бюджетного процесса** в соответствии с настоящей заявкой (Приложения ____ шт):

Номер приложения к Заявке на подключение	**ФИО пользователя**

Руководитель организации /Уполномоченное лицо организации _____
(должность) (подпись) (ФИО полностью)

М.П.

« » _____ 20 __ г.

Приложение №____
к Заявке на подключение к компонентам
системы «Электронный бюджет»
для ведения реестра участников
бюджетного процесса

ФИО пользователя	
СНИЛС	
Должность	
Подразделение	
Информация о сертификате	*<указывается наименование файла сертификата пользователя, предоставляемого совместно с заявкой на подключение>*

Полномочие			
Ввод данных	**Согласование**	**Утверждение**	**Просмотр**
Добавить/ Исключить	*Добавить/ Исключить*	*Добавить/ Исключить*	*Добавить/ Исключить*

☐ Прекращение доступа пользователя к системе

Заполняется в случае необходимости прекратить доступ пользователя к системе

Сотрудник организации
(пользователь) _____
(подпись) (расшифровка подписи)

Руководитель организации
/Уполномоченное лицо
организации _____
(подпись) (расшифровка подписи)

М.П.

Приложение № 2
к письму Министерства финансов
Российской Федерации
от «___»_____2015 г. № _____

ЗАЯВКА
на выдачу СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ[1]

(наименование органа Федерального казначейства)

от «__» _____ 20__ г. №_____

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)

[1] Оформляется на бланке письма организации

Приложение № 3
к письму Министерства финансов
Российской Федерации
от «___»_____2015 г. № _____

Примерная форма[1]

Доверенность № ____

«____»_____20____г.

_____
(организация)

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)

Приложение № 4
к письму Министерства финансов
Российской Федерации
от «___»_____2015 г. № _____

Перечень мероприятий,
которые необходимо выполнить Уполномоченной организации для
подключения к компонентам системы «Электронный бюджет»

1. Подготовка информационно-технологической инфраструктуры к подключению к компонентам системы «Электронный бюджет».

При подготовке информационно-технологической инфраструктуры к подключению Уполномоченной организации необходимо провести следующие мероприятия:

а) определить ответственного за техническое обеспечение работы с компонентами системы «Электронный бюджет» и подключение пользователей;

б) оформить доверенность на получение специальных средств криптографической защиты информации, обеспечивающих создание защищенного соединения с компонентами системы «Электронный бюджет» (далее – СКЗИ), лицензионных ключей и эксплуатационной документации к СКЗИ ответственному за техническое обеспечение работы с компонентами системы «Электронный бюджет» и подключение пользователей;

в) направить в орган Федерального казначейства заявку о выдаче СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ. Заявка о выдаче СКЗИ, лицензионных ключей и эксплуатационной документации к СКЗИ предоставляется одновременно с заявкой на подключение к компонентам системы «Электронный бюджет»;

г) получить СКЗИ, лицензионные ключи и эксплуатационную документацию к СКЗИ в органе Федерального казначейства;

д) обеспечить соответствие автоматизированных рабочих мест пользователей требованиям к автоматизированному рабочему месту, с которого осуществляется доступ к компонентам системы «Электронный бюджет» (приложение № 1 к настоящему Перечню), включая установку и настройку СКЗИ на автоматизированных рабочих местах пользователей;

е) выполнить требования по обеспечению информационной безопасности автоматизированного рабочего места, с которого осуществляется доступ к компонентам системы «Электронный бюджет» (приложение № 2 к настоящему Перечню).

2. Мероприятия по подключению пользователей.

Для подключения пользователей к компонентам системы «Электронный бюджет» Уполномоченной организации необходимо провести следующие мероприятия:

а) определить ответственных за ведение реестра участников бюджетного процесса;

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

в) представить в МОУ Федерального казначейства по месту нахождения организации соответствующие заявки на подключение к компонентам системы «Электронный бюджет», подписанные руководителем (заместителем руководителя) или иным уполномоченным лицом Уполномоченной организации, на бумажном носителе в двух экземплярах (заявки представляются ответственным за техническое обеспечение работы с компонентами системы «Электронный бюджет» и подключение пользователей).

Одновременно с заявкой на подключение к компонентам системы «Электронный бюджет» в орган Федерального казначейства предоставляются:

документ, подписанный руководителем, определяющий ответственного за техническое обеспечение работы с компонентами системы «Электронный бюджет» и подключение пользователей (представляется однократно);

заверенная в установленном порядке копия распорядительного документа или доверенность, подтверждающие право уполномоченного лица действовать от имени Уполномоченной организации, в случае если заявка на подключение к компонентам системы «Электронный бюджет» подписана не руководителем (заместителем руководителя) Уполномоченной организации, а иным уполномоченным лицом Уполномоченной организации;

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

согласие на обработку персональных данных каждого подключаемого пользователя (приложение № 3 к настоящему Перечню).

3. Мероприятия, проводимые органом Федерального казначейства, при рассмотрении заявки на подключение к компонентам системы «Электронный бюджет».

Орган Федерального казначейства в течение 3 (трех) рабочих дней со дня предоставления заявки на подключение к компонентам системы «Электронный бюджет» осуществляет проверку ее содержания на:

соответствие заявки на подключение к компонентам системы «Электронный бюджет» установленной форме;

наличие действующего на момент рассмотрения заявки на подключение к компонентам системы «Электронный бюджет» сертификата пользователя, включенного в Заявку на подключение;

идентичность сведений о пользователе, указанных в заявке на подключение к компонентам системы «Электронный бюджет», соответствующим сведениям в предоставленном сертификате;

наличие документов, указанных в пункте 2 настоящего Перечня.

По результатам проверки заявки на подключение к компонентам системы «Электронный бюджет» и сертификата орган Федерального казначейства формирует информацию о результатах проверки отдельно по каждому пользователю, указанному в заявке на подключение к компонентам системы «Электронный бюджет».

В случае положительного результата проверки заявки на подключение к компонентам системы «Электронный бюджет» орган Федерального казначейства на основании сведений, содержащихся в заявке на подключение к компонентам системы «Электронный бюджет», предоставляет Уполномоченной организации и пользователям доступ к компонентам системы «Электронный бюджет».

Не позднее 2 (двух) рабочих дней со дня предоставления доступа пользователю к компонентам системы «Электронный бюджет» орган Федерального казначейства уведомляет ответственного за техническое обеспечение работы с компонентами системы «Электронный бюджет» 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 к компонентам системы «Электронный бюджет» (приложение № 4 к настоящему Перечню).

В случае отрицательного результата проверки заявки на подключение к компонентам системы «Электронный бюджет» доступ пользователю к компонентам системы «Электронный бюджет» не предоставляется и орган Федерального казначейства не позднее 2 (двух) рабочих дней после проверки заявки на подключение к компонентам системы «Электронный бюджет»

уведомляет ответственного за техническое обеспечение работы с компонентами системы «Электронный бюджет» и подключение пользователей об отказе в предоставлении доступа к компонентам 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 к компонентам системы «Электронный бюджет» (приложение № 4 к настоящему Перечню).

Приложение № 1
к Перечню мероприятий,
которые необходимо выполнить
федеральным органам государственной
власти для подключения к компонентам
системы «Электронный бюджет»

Требования к автоматизированному рабочему месту, с которого осуществляется доступ к компонентам системы «Электронный бюджет»

В целях подключения к компонентам системы «Электронный бюджет» автоматизированное рабочее место (далее – АРМ пользователя) должно соответствовать следующим техническим требованиям:

1. Минимальные аппаратные характеристики АРМ пользователя компонентов системы «Электронный бюджет» приведены в таблице 1.

Таблица 1. Минимальные аппаратные характеристики АРМ пользователя.

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 пользователя:

- 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 пользователя:

- 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 компонентами «Электронный бюджет» могут быть использованы следующие носители ключевой информации сертификата пользователя:

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

Приложение № 2
к Перечню мероприятий,
которые необходимо выполнить
федеральным органам государственной
власти для подключения к компонентам
системы «Электронный бюджет»

Требования по обеспечению информационной безопасности автоматизированного рабочего места, с которого осуществляется доступ к компонентам системы «Электронный бюджет»

1. В настоящем приложении используются следующие термины и сокращения:

АО – аппаратное обеспечение;

АРМ – автоматизированное рабочее место пользователя компонентов системы «Электронный бюджет»;

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 пользователя, должен быть назначен администратор информационной безопасности, на которого возлагаются задачи организации работ по использованию АРМ пользователя,

выработки соответствующих инструкций для пользователей, а также контроль за соблюдением описанных ниже требований.

4. При размещении технических средств с установленным АРМ пользователя:

должны быть приняты меры по исключению НСД в помещения, в которых размещены технические средства с установленным АРМ пользователя, 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 исполнителям работ 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 пользователя необходимо соблюдать следующие требования:

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

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

3) на АРМ пользователя 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 пользователя (например, путем опечатывания системного блока и разъемов АРМ пользователя);

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

6) ПО, устанавливаемое на АРМ пользователя, 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 пользователя, если во время его начальной загрузки не проходят встроенные тесты;

3) запрещается:

– оставлять без контроля вычислительные средства, на которых эксплуатируется АРМ пользователя, 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 пользователя, 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 её настроек;

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

– всем пользователям 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 пользователей.

7. Для работы АРМ пользователя с компонентами системы «Электронный бюджет» 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 пользователя;

– 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.

Пользователь 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 пользователь АРМ должен 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 пользователь АРМ должен немедленно прекратить работу и сообщить об этом руководителю и администратору информационной безопасности (или сотруднику, выполняющему эти функции).

Правила и рекомендации пользователю АРМ 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) проводит пользователь при первом применении носителя на данном компьютере. Последующие контроли носителя производить перед каждым просмотром состава и содержимого файлов;

– в целях исключения автозапуска исполняемых файлов со сменных носителей (CD, DVD, USB флеш-накопителей и т.п.) пользователю 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 пользователя с компонентами системы «Электронный бюджет» 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 пользователя, зависит от способа взаимодействия АРМ пользователя с компонентами системы «Электронный бюджет». По способу взаимодействия с компонентами системы «Электронный бюджет» АРМ пользователя подразделяется на следующие типы:

- Тип 1 - АРМ, взаимодействующий с компонентами системы «Электронный бюджет» посредством прямого подключения к сети Интернет.
- Тип 2 - АРМ, взаимодействующий с компонентами системы «Электронный бюджет» посредством подключения к сети Интернет через ЛВС организации.
- Тип 3 - АРМ, взаимодействующий с компонентами системы «Электронный бюджет» посредством подключения по выделенным каналам связи через ЛВС организации.

11. Взаимодействие АРМ Тип 1 с компонентами системы «Электронный бюджет» 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 с компонентами системы «Электронный бюджет», объектами ЛВС организации и ресурсами сети Интернет 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 автоматизированное рабочее место пользователя компонентов системы «Электронный бюджет» 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 компонентам системы «Электронный бюджет», 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 № 3
к Перечню мероприятий,
которые необходимо выполнить
федеральным органам государственной
власти для подключения к компонентам
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_____№_____ дата выдачи_____ название выдавшего органа _____, в соответствии с требованиями статьи 9 Федерального закона от 27.07.2006 № 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 системе 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 № 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 № 4
к Перечню мероприятий,
которые необходимо выполнить
федеральным органам государственной
власти для подключения к компонентам
системы «Электронный бюджет»

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

Результат отработки:

Наименование организации _____

Приложение №___ _____
Приложение №___ _____
_____
<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.