**Типовые требования**

**для включения в описание объектов закупки при заключении государственных и муниципальных контрактов**

**на создание и сопровождение информационных систем всех типов**

**2024 г.**

**Содержание**

[I. Типовые требования для включения в описание объектов закупки при заключении государственных и муниципальных контрактов на создание информационных систем всех типов 3](#__RefHeading___1)

[Требования к Системе в части поддержки отечественного программного обеспечения 3](#__RefHeading___2)

[Требования к подсистеме идентификации и аутентификации субъектов доступа и объектов доступа в Системе 3](#__RefHeading___3)

[Требования к подсистеме регистрации событий безопасности в Системе 4](#__RefHeading___4)

[Требования к защите информации о событиях безопасности 4](#__RefHeading___5)

[Требования к управлению пользовательскими паролями 5](#__RefHeading___6)

[Требования к контролю, хранению, обновлению и восстановлению данных 5](#__RefHeading___7)

[Требования к защите информации исполнителем 5](#__RefHeading___8)

[Требования к конфиденциальности информации 7](#__RefHeading___9)

[II. Типовые требования для включения в описание объектов закупки при заключении государственных и муниципальных контрактов на сопровождение информационных систем всех типов 8](#__RefHeading___10)

[Требования к Системе в части поддержки отечественного программного обеспечения 8](#__RefHeading___11)

[Требования к защите информации исполнителем 8](#__RefHeading___12)

[Требования к конфиденциальности информации 10](#__RefHeading___13)

# **I. Типовые требования для включения в описание объектов закупки** **при заключении государственных и муниципальных контрактов** **на создание информационных систем всех типов**

(далее - Система)

**Требования к Системе в части поддержки**
**отечественного программного обеспечения**

Для надежности Системы, в срок не более 20 рабочих дней, должно быть обеспечено своевременное тестирование и совместимость:

* работоспособности Системы с официальными релизами и версиями ядер операционных систем на базе Astra Linux (поддержка как графических, так
и командных интерфейсов для эффективного взаимодействия с системными ресурсами), с дальнейшим обновлением. В случае несовместимости Системы
с отдельными компонентами, входящими в состав официального релиза операционной системы, необходимо провести всесторонний анализ всех установленных библиотек и программных модулей, определить, какие именно версии или компоненты обладают необходимыми функциями, и осуществить доработку Системы для ее стабильной работы с обновленной операционной системой.
* системы антивирусной защиты информации Dr.Web, включая регулярные обновления, которые должны обеспечивать высокий уровень защиты от угроз и уязвимостей (без нарушения производительности компонентов Системы);
* системы защиты информации от несанкционированного доступа Secret Net Studio для Linux/Secret Net LSP, которая должна включать в себя механизмы шифрования данных и аутентификации пользователей (стабильная
и безопасная среда для работы пользователей, минимизируя риски потерь
и несанкционированного доступа к информации).

Результатом тестирования должен быть Протокол тестирования обновлений.

**Требования к подсистеме идентификации и аутентификации**
**субъектов доступа и объектов доступа в Системе**

Система должна предусматривать следующие функции:

- идентификацию и аутентификацию субъектов доступа на основе паролей (аутентификационной информации);

- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов;

- управление аутентификационной информацией, в том числе хранение, выдачу, инициализацию, принудительное блокирование;

- управление ролями доступа субъектов доступа посредством Системы
к объектам доступа;

- реализацию ролевого метода разграничения доступа в Системе;

- управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами;

- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование Cистемы;

- назначение необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование Cистемы;

- блокирование сеанса доступа в Cистему после установленного времени бездействия (неактивности) пользователя или по его запросу;

- запрет действий пользователей, разрешенных до идентификации
и аутентификации.

Вся аутентификационная информация должна обрабатываться и храниться в базе данных Системы в зашифрованном виде с использованием средств криптографической защиты информации Заказчика.

**Требования к подсистеме регистрации событий безопасности**
**в Системе**

Система должна осуществлять регистрацию событий безопасности, их запись и хранение течение установленного времени.

Система должна регистрировать события безопасности, содержащие, как минимум:

* данные о создании, удалении, блокировке идентификатора пользователя;
* данные о назначении, изменении ролей, прав пользователя;
* данные о входе (выходе) в Систему (из Системы);
* данные о результате попытке входа (успешной или неуспешной), идентификатор, предъявленный при доступе или попытке доступа;
* данные о дате и времени для каждого регистрируемого события;

Объем и срок хранения событий безопасности должены быть настраиваемыми.

Система должна использовать системное время операционной системы, под управлением которой она функционирует.

**Требования к защите информации о событиях безопасности**

Для доступа к данным и функциям Системы сотрудники должны пройти процедуру аутентификации посредством ввода пары логин/пароль
в специальном диалоговом окне входа. Допускается подключение функционала для авторизации пользователей с использованием ЕСИА для иных пользователей.

При идентификации пользователей по логину/паролю должен быть реализован механизм запроса согласия на обработку персональных данных
по заданному шаблону Заказчика. В случае согласия авторизация пользователя допускается, в случае отказа – отказ в авторизации пользователя.

Доступ к данным и функциям Системы должен предоставляться
на основании авторизации пользователя и его роли.

**Требования к управлению пользовательскими паролями**

Регистрацию новых пользователей, блокировку пользователей и сброс забытых паролей осуществляют только администраторы.

Процедура хранения и выдачи пароля новым пользователям должна быть организована таким образом, чтобы действительный пароль для доступа
к Системе знал только сам пользователь (например, вход по одноразовому паролю с обязательной последующей его заменой). При создании пользователя ему назначается временный пароль, который он обязан заменить при первой попытке входа.

На пользовательские пароли должны накладываться настраиваемые ограничения по минимальной длине и сложности:

1. минимальное количество символов: 8;
2. пароль должен включать:

латинские буквы верхнего и нижнего регистра (A-Z, a-z);

цифры (0-9);

специальные символы.

Должен быть реализован механизм «Требование смены пароля при первом входе».

В Системе должен быть реализован механизм восстановления пароля.

**Требования к контролю, хранению, обновлению**
**и восстановлению данных**

В Системе должна поддерживаться логическая целостность данных, то есть изменения должны носить характер транзакционно-ориентированных, выполняющихся в целом от начала до конца либо, в случае сбоя,
не выполняющихся совсем.

Должны обеспечиваться сохранность и целостность данных Системы,
а также выполнение комплекса мер по резервному копированию данных. Средства резервного копирования предоставляются Заказчиком.

В целях обеспечения безопасности данных и защиты конфиденциальной информации запрещено резервное копирование Системы на собственные мощности Подрядчика без согласования с Заказчиком (оператором владельца).

**Требования к защите информации исполнителем**

Доступ осуществляется через защищенную сеть передачи данных.
К вычислительным мощностям доступ предоставляется при наличии
у Исполнителя необходимых технических и программных средств для защиты информации при подключении к сети Заказчика. Подключение к защищенной сети Заказчика, а также приобретение необходимых лицензий и дистрибутивов выполняются за счет Исполнителя.

Средства криптографической защиты информации необходимо использовать не ниже класса КС3 с действующим сертификатом ФСБ России:

* Программный комплекс ViPNet Client (версия не ниже 4.5)
для сети № 2301;
* Программный комплекс ViPNet Client 4U for Linux для сети № 2301;
* Средство криптографической защиты информации «Континент-АП» (версия не ниже 4);
* Программно-аппаратный комплекс ViPNet Coordinator HW 4;
* Аппаратно-программный комплекс шифрования «Континент» (версия не ниже 3.9).

Требования для подключения к защищенной сети Заказчика размещены на официальном сайте https://digital42.ru в разделе «Документы» пункт меню «Информационная безопасность».

Для удаленного оказания услуг Исполнитель обязан подключиться
к защищенной сети передачи данных (сеть ViPNet  № 2301 или «Континент») оператора центра обработки данных информационных систем Кемеровской области – Кузбасса (далее – оператор ЦОД) с соблюдением требований законодательства Российской Федерации. Оператор ЦОД – Министерство цифрового развитии связи Кузбасса.

Для подключения к защищенной сети передачи данных оператора ЦОД, Исполнитель заключает соответствующие соглашения по типовой форме через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru).

При организации подключения удаленных рабочих мест Исполнителя
на автоматизированных местах должны быть выполнены все требования по обеспечению защиты информации в государственных информационных системах в соответствии с законодательством Российской Федерации. Исполнителем подается заявка оператору ЦОД с указанием следующих данных:

* фамилия, имя, отчество (при наличии) пользователя (ей) автоматизированного рабочего места;
* должность;
* контактный номер телефона;
* адрес электронной почты;
* скан-копия согласия на обработку персональных данных;
* адрес размещения автоматизированного рабочего места;
* номер, дата и наименование государственного контракта;
* MAC-адрес автоматизированного рабочего места;
* инвентарный номер (в соответствии с бухгалтерским учетом Исполнителя);
* наименование сопровождаемой информационной системы;
* IP адрес(а) серверных мощностей, на которых будет/размещена информационная система;
* номер порта(ов) доступа;
* наименование протокола доступа;
* документ, подтверждающий установку средств защиты информации
с указанием версии и номера сертификата ФСТЭК России и/или ФСБ России: средства криптографической защиты информации, средство межсетевого экранирования, средство защиты информации от несанкционированного действия, средство антивирусной защиты информации на указанное автоматизированное рабочее место.

Подача заявки осуществляется через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru), услуга «Подключение подрядной организации к инфраструктуре Центра обработки данных информационных систем Кемеровской области - Кузбасса».

После проверки предоставленных документов оператором ЦОД не позднее 5-ти рабочих дней создаются учетные данные для доступа и передаются
по электронной почте, указанной в заявке.

В случае невозможности выполнить требования на автоматизированных рабочих местах Исполнителя, услуги оказываются без использования дистанционных технологий, по месту нахождения Заказчика.

При необходимости оказания услуг вне рабочего времени все виды работы
и время согласовываются с Заказчиком и оператором ЦОД, при этом начало работ не должно превышать одного часа после обращения (заявки) Заказчика.

Исполнитель обязан обрабатывать запрос на устранение уязвимостей в ПО по запросу Заказчика и/или оператора ЦОД.

**Требования к конфиденциальности информации**

Подрядчик обязан соблюдать конфиденциальность информации, ставшей ему известной в ходе исполнения Контракта, не передавать третьим лицам и не раскрывать публично конфиденциальную информацию без согласия Заказчика,
а также соблюдать требования к защите указанной информации, предусмотренные действующим законодательством.

К конфиденциальной информации относится любая информация
в бумажной или электронной форме, предоставленная Заказчиком Подрядчику
в процессе выполнения обязательств по Контракту.

К конфиденциальной информации не относится информация, которая отнесена законодательством Российской Федерации к категории открытой
и раскрытие которой вменено в обязанность Заказчику или Подрядчику.

Подрядчик имеет право предоставлять доступ к конфиденциальной информации своим сотрудникам для выполнения ими своих трудовых обязанностей при условии соблюдения ее конфиденциальности.

Подрядчик не несет ответственности за разглашение полученной конфиденциальной информации, если она:

* на момент раскрытия была общеизвестной;
* была самостоятельно разработана Подрядчиком;
* раскрыта государственным органам в соответствии с действующим законодательством Российской Федерации;
* предоставлена Заказчиком третьей стороне до момента подписания Контракта.

# **II. Типовые требования для включения в описание объектов закупки при заключении государственных и муниципальных контрактов на сопровождение информационных систем всех типов**

(далее - Система)

**Требования к Системе в части поддержки**
**отечественного программного обеспечения**

Для надежности Системы, в срок не более 20 рабочих дней, должно быть обеспечено своевременное тестирование и совместимость:

* работоспособности Системы с официальными релизами и версиями ядер операционных систем на базе Astra Linux (поддержка как графических, так
и командных интерфейсов для эффективного взаимодействия с системными ресурсами), с дальнейшим обновлением. В случае несовместимости Системы
с отдельными компонентами, входящими в состав официального релиза операционной системы, необходимо провести всесторонний анализ всех установленных библиотек и программных модулей, определить, какие именно версии или компоненты обладают необходимыми функциями, и осуществить доработку Системы для ее стабильной работы с обновленной операционной системой.
* системы антивирусной защиты информации Dr.Web, включая регулярные обновления, которые должны обеспечивать высокий уровень защиты от угроз и уязвимостей (без нарушения производительности компонентов Системы);
* системы защиты информации от несанкционированного доступа Secret Net Studio для Linux/Secret Net LSP, которая должна включать в себя механизмы шифрования данных и аутентификации пользователей (стабильная
и безопасная среда для работы пользователей, минимизируя риски потерь
и несанкционированного доступа к информации).

Результатом тестирования должен быть Протокол тестирования обновлений.

**Требования к защите информации исполнителем**

Доступ осуществляется через защищенную сеть передачи данных.
К вычислительным мощностям доступ предоставляется при наличии
у Исполнителя необходимых технических и программных средств для защиты информации при подключении к сети Заказчика. Подключение к защищенной сети Заказчика, а также приобретение необходимых лицензий и дистрибутивов выполняются за счет Исполнителя.

Средства криптографической защиты информации необходимо использовать не ниже класса КС3 с действующим сертификатом ФСБ России:

* Программный комплекс ViPNet Client (версия не ниже 4.5)
для сети № 2301;
* Программный комплекс ViPNet Client 4U for Linux для сети № 2301;
* Средство криптографической защиты информации «Континент-АП» (версия не ниже 4);
* Программно-аппаратный комплекс ViPNet Coordinator HW 4;
* Аппаратно-программный комплекс шифрования «Континент» (версия не ниже 3.9).

Требования для подключения к защищенной сети Заказчика размещены на официальном сайте https://digital42.ru в разделе «Документы» пункт меню «Информационная безопасность».

Для удаленного оказания услуг Исполнитель обязан подключиться
к защищенной сети передачи данных (сеть ViPNet  № 2301 или «Континент») оператора центра обработки данных информационных систем Кемеровской области – Кузбасса (далее – оператор ЦОД) с соблюдением требований законодательства Российской Федерации. Оператор ЦОД – Министерство цифрового развитии связи Кузбасса.

Для подключения к защищенной сети передачи данных оператора ЦОД, Исполнитель заключает соответствующие соглашения по типовой форме через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru).

При организации подключения удаленных рабочих мест Исполнителя
на автоматизированных местах должны быть выполнены все требования по обеспечению защиты информации в государственных информационных системах в соответствии с законодательством Российской Федерации. Исполнителем подается заявка оператору ЦОД с указанием следующих данных:

* фамилия, имя, отчество (при наличии) пользователя (ей) автоматизированного рабочего места;
* должность;
* контактный номер телефона;
* адрес электронной почты;
* скан-копия согласия на обработку персональных данных;
* адрес размещения автоматизированного рабочего места;
* номер, дата и наименование государственного контракта;
* MAC-адрес автоматизированного рабочего места;
* инвентарный номер (в соответствии с бухгалтерским учетом Исполнителя);
* наименование сопровождаемой информационной системы;
* IP адрес(а) серверных мощностей, на которых будет/размещена информационная система;
* номер порта(ов) доступа;
* наименование протокола доступа;
* документ, подтверждающий установку средств защиты информации
с указанием версии и номера сертификата ФСТЭК России и/или ФСБ России: средства криптографической защиты информации, средство межсетевого экранирования, средство защиты информации от несанкционированного действия, средство антивирусной защиты информации на указанное автоматизированное рабочее место.

Подача заявки осуществляется через информационную систему «Реестр государственных информационных систем Кемеровской области – Кузбасса» (ris.kemobl.ru), услуга «Подключение подрядной организации к инфраструктуре Центра обработки данных информационных систем Кемеровской области - Кузбасса».

После проверки предоставленных документов оператором ЦОД не позднее 5-ти рабочих дней создаются учетные данные для доступа и передаются
по электронной почте, указанной в заявке.

В случае невозможности выполнить требования на автоматизированных рабочих местах Исполнителя, услуги оказываются без использования дистанционных технологий, по месту нахождения Заказчика.

При необходимости оказания услуг вне рабочего времени все виды работы
и время согласовываются с Заказчиком и оператором ЦОД, при этом начало работ не должно превышать одного часа после обращения (заявки) Заказчика.

Исполнитель обязан обрабатывать запрос на устранение уязвимостей в ПО по запросу Заказчика и/или оператора ЦОД.

**Требования к конфиденциальности информации**

Подрядчик обязан соблюдать конфиденциальность информации, ставшей ему известной в ходе исполнения Контракта, не передавать третьим лицам и не раскрывать публично конфиденциальную информацию без согласия Заказчика,
а также соблюдать требования к защите указанной информации, предусмотренные действующим законодательством.

К конфиденциальной информации относится любая информация
в бумажной или электронной форме, предоставленная Заказчиком Подрядчику
в процессе выполнения обязательств по Контракту.

К конфиденциальной информации не относится информация, которая отнесена законодательством Российской Федерации к категории открытой
и раскрытие которой вменено в обязанность Заказчику или Подрядчику.

Подрядчик имеет право предоставлять доступ к конфиденциальной информации своим сотрудникам для выполнения ими своих трудовых обязанностей при условии соблюдения ее конфиденциальности.

Подрядчик не несет ответственности за разглашение полученной конфиденциальной информации, если она:

* на момент раскрытия была общеизвестной;
* была самостоятельно разработана Подрядчиком;
* раскрыта государственным органам в соответствии с действующим законодательством Российской Федерации;
* предоставлена Заказчиком третьей стороне до момента подписания Контракта.