

**ИНФОРМАЦИОННАЯ СИСТЕМА
«УДОСТОВЕРЯЮЩИЙ ЦЕНТР
ФЕДЕРАЛЬНОГО КАЗНАЧЕЙСТВА»**

Требования по информационной безопасности к
рабочему месту оператора доверенного лица
Удостоверяющего центра Федерального казначейства

Код документа: 40308570.34.99,99,ДР.022-01.00 1

Листов: 4

Наименование ИС:	Информационная система «Удостоверяющий центр Федерального казначейства»	
Название документа	Требования по информационной безопасности к рабочему месту оператора доверенного лица	
Код документа:	40308570.34.99,99.ДР.022-01.00 1	Стр. 2

Аннотация

Настоящий документ содержит требования по информационной безопасности, предъявляемые со стороны Удостоверяющего центра Федерального казначейства, к рабочим местам операторов доверенных лиц (далее – ДЛ) Удостоверяющего центра Федерального казначейства (далее – УЦ ФК).

Наименование ИС:	Информационная система «Удостоверяющий центр Федерального казначейства»	
Название документа	Требования по информационной безопасности к рабочему месту оператора доверенного лица	
Код документа:	40308570.34.99,99.ДР.022-01.00 1	Стр. 3

Перечень сокращений

Термины и сокращения	Содержание
АРМ	Автоматизированное рабочее место
ДЛ	Доверенное лицо
ИБ	Информационная безопасность
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПО	Программное обеспечение
СКЗИ	Средства криптографической защиты информации
УЦ	Удостоверяющий центр
ФК	Федеральное казначейство
ФСБ России	Федеральная служба безопасности Российской Федерации

Наименование ИС:	Информационная система «Удостоверяющий центр Федерального казначейства»	
Название документа	Требования по информационной безопасности к рабочему месту оператора доверенного лица	
Код документа:	40308570.34.99,99.ДР.022-01.00 1	Стр. 4

1 Требования по информационной безопасности

В качестве криптографического провайдера на АРМ операторов ДЛ должно использоваться сертифицированное ФСБ России СКЗИ «КриптоПро CSP 4.0» (класса КС2) и выполняться все требования, перечисленные в его правилах пользования и формуляре.

Использование СКЗИ класса КС2 возможно только совместно с аппаратным датчиком случайных чисел и аппаратно-программным модулем доверенной загрузки (например, ПАК «Соболь» 3.x с сертификатом ФСБ России).

В дополнение должны выполняться следующие требования:

- должны быть установлены все актуальные патчи безопасности ОС и ПО, установленных на АРМ;
- должно использоваться только лицензионное ПО;
- должны быть установлены средства антивирусной защиты:
 - обновление сигнатур антивирусных баз должно выполняться по расписанию ежедневно;
 - задача сканирования файловой системы на предмет наличия вредоносного ПО должна выполняться по расписанию ежедневно.
- АРМ операторов ДЛ должны размещаться в пределах контролируемой зоны организации;
- Все пароли, используемые на АРМ, должны удовлетворять следующим требованиям:
 - длина пароля не менее восьми символов;
 - мощность алфавита не менее 36 символов;
 - срок смены пароля не реже одного раза в три месяца;
 - учетная запись должна блокироваться на срок не менее десяти минут при трёх неуспешных попытках ввода пароля.
 - доступ к паролю должен быть обеспечен только сотруднику, обладающему правами на доступ в Систему от имени соответствующей паролю учетной записи.
 - Предусмотреть меры, исключающие возможность несанкционированного не обнаруживаемого изменения аппаратной части технических средств