

Утверждены
решением Правления
Федеральной нотариальной палаты
От 23.03.2020 г., протокол №04/20

РЕКОМЕНДАЦИИ ПО ОБОРУДОВАНИЮ И ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ ДЛЯ НОТАРИАЛЬНОЙ КОНТОРЫ

Рекомендации для пользователей

Версия 1.1

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 2

СОДЕРЖАНИЕ

1	Термины и определения	3
2	Общие положения	4
3	Средства межсетевого взаимодействия	4
4	Средства обеспечения информационной безопасности	6
4.1	Средства разграничения и контроля доступа	6
4.2	Выполнение требований законодательства РФ в области обработки и защиты персональных данных	7
4.3	Антивирусная защита	8
4.4	Защита информации от утечек	8
4.5	Межсетевое экранирование	9
4.6	Резервное копирование	9
4.6.1	Ручной режим	9
4.6.2	Автоматизированный режим	9
5	Аппаратное обеспечение	9
6	Программное обеспечение	13

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 3

1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Таблица 1. Термины и определения

Термины и сокращения	Определения
ЕИС	Единая информационная система нотариата
Защита информации (ЗИ)	Деятельность, направленная на предотвращение утечки защищаемой информации, а также несанкционированных и непреднамеренных воздействий на нее.
Криптографическая защита информации	Защита информации с использованием криптографических средств
Локальный сервер	Компьютер, на котором установлена СУБД ЕИС, и который выполняет обмен с сервером ЕИС
Общесистемное программное обеспечение, ОС	Операционная система. Базовый комплекс программ, обеспечивающий управление аппаратными средствами компьютера, работу с файлами, ввод и вывод данных, а также выполнение прикладных программ и утилит.
ОС	Операционная система
ПАК	Программно-аппаратный комплекс
ПК	Персональный компьютер
ПО	Программное обеспечение
Прикладное программное обеспечение	Программное обеспечение, предназначенное для автоматизации нотариальной деятельности и рассчитанное на непосредственное взаимодействие с пользователем
Провайдер	Поставщик услуг связи с сетью «Интернет»
СЗИ	Средство защиты информации (в том числе СКЗИ)
СКЗИ	Средство криптографической защиты информации, в том числе средства шифрования, имитозащиты, электронной подписи, кодирования, изготовления ключевых документов, ключевые документы.
Специализированное программное обеспечение	Программное обеспечение, выполняющее задачи по обеспечению информационной безопасности (антивирусная защита, криптографическая защита, резервное копирование, разграничение доступа, предотвращение утечек информации, межсетевое экранирование), организации межсетевого взаимодействия и т.д.
СУБД	Система управления базами данных
Угроза (безопасности информации)	Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.
ФНП	Федеральная нотариальная палата
ФЦИИТ	Фонд «Центр инноваций и информационных технологий»
VDI	Virtual Desktop Infrastructure – инфраструктура виртуальных машин для работы сотрудников на локальном сервере
WAN	Wide Area Network – глобальная сеть (Интернет)
WWAN	Wireless Wide Area Network – беспроводное (через сети сотовой связи) подключение к сети Интернет

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 4



Рекомендации, приведенные в настоящем документе, не являются обязательными и носят информационно-справочный характер.

2 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящие «Рекомендации по оборудованию и программному обеспечению для нотариальной конторы» (далее - Рекомендации) разработаны Фондом «Центр инноваций и информационных технологий» Федеральной нотариальной палаты с целью:

- повышения уровня осведомленности пользователей о рекомендуемых характеристиках оборудования для работы с ЕИС;
- оптимизации временных затрат по выбору программно-аппаратных решений при осуществлении нотариальной деятельности;
- актуализации рекомендаций Фонда по обеспечению информационной безопасности.

Рекомендации предназначены для нотариусов и сотрудников нотариальных палат субъектов РФ, являющихся пользователями ЕИС.

3 СРЕДСТВА МЕЖСЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

Для осуществления информационного обмена с сервером ЕИС необходимо подключение к сети Интернет. Рекомендуется осуществлять подключение посредством маршрутизаторов.

При выборе поставщика услуг связи (провайдера) рекомендуется учитывать:

- Деловую репутацию организации: опыт работы на рынке, спектр предоставляемых услуг, отзывы пользователей.
- Наличие и круглосуточную доступность службы технической поддержки пользователей.
- Возможность отличия фактической скорости передачи данных от предусмотренной договором в зависимости от внешних факторов.
- Тип подключения.



Для обеспечения стабильной работы ЕИС рекомендуется резервировать канал связи с сетью Интернет при помощи радиоканала (мобильной или спутниковой связи) или второго проводного канала, подключенного к другому провайдеру.

Приоритетность типов подключений:

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 5

Подключение по выделенной линии (витая пара или оптоволоконная сеть). Обеспечивает, как правило, наиболее высокую надежность соединения и скорость передачи данных. Рекомендуется для основного канала.

Подключение через телевизионный кабель. Использует модем типа DOCSIS. Позволяет обеспечить достаточную надежность соединения и скорость передачи данных.

Подключение через телефонную линию (DSL). Скорость передачи данных и надежность соединения существенно зависят от состояния местной телефонной сети.

Подключение через сети сотовой связи. Обеспечивается маршрутизаторами с модулем сотовой связи (4G) или USB-модемами. Менее стабильно, чем проводное подключение. Рекомендуется в качестве резервного канала при отсутствии технической или финансовой возможности подключения двух независимых выделенных линий.

Спутниковый интернет. Позволяет обеспечить достаточную надежность соединения, но имеет ряд недостатков: сложность с настройкой и установкой оборудования, высокая стоимость услуг.

При наличии в нотариальной конторе локальной сети, рекомендуется применение маршрутизатора с модулем сотовой связи (4G, WWAN) или двумя интернет-подключениями (Dual-WAN). Такие маршрутизаторы обеспечивают непрерывное подключение для всей локальной сети при потере одного из каналов.

При реализации резервного канала с помощью сотовой связи, рекомендуется подключение 4G-модема к маршрутизатору с помощью USB-порта, для поддерживающих передачу данных через USB-порт моделей. В остальных случаях резервный канал следует подключать к выполняющему роль локального сервера ЕИС компьютеру.



Для стабильной работы видеоконференцсвязи при совершении нотариальных действий необходима скорость передачи данных не менее 1 Мбит/с. При высокой нагрузке на сеть и видеосвязи в разрешении 1920x1080 рекомендуется скорость передачи данных 10 Мбит/с для основного канала.

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 6

4 СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Средства разграничения и контроля доступа

В целях предотвращения несанкционированного доступа посторонних лиц к информационным ресурсам ЕИС рекомендуется применять:

- Штатные средства операционной системы – защиту учетных записей пользователей паролем.
- Специальные программные и/или программно-технические комплексы, осуществляющие дополнительные меры по аутентификации и контролю доступа: сертифицированный аппаратно-программный модуль доверенной загрузки, сертифицированное средство защиты информации от несанкционированного доступа.



В целях предотвращения несанкционированных действий не рекомендуется:

1. Работать в ЕИС под учетной записью пользователя операционной системы Microsoft Windows с правами администратора;
2. Оставлять без защиты паролем (с «пустым паролем») учетные записи пользователей и администраторов операционной системы.

Для предотвращения компрометации паролей следует учитывать следующие правила:

Правила формирования пароля:

- 1) Для разных подсистем должны использоваться разные пароли.
- 2) Пароль не должен содержать:
 - имя учетной записи пользователя или какую-либо его часть;
 - имена и даты рождения пользователя и его родственников;
 - клички домашних животных, номера автомобилей, телефонов и иную известную другим лицам информацию о пользователе;
 - один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;
 - комбинации символов, набираемых в закономерном порядке на клавиатуре (например, 1234567);
 - пароли, которые уже использовались ранее.
- 3) Пароль должен состоять не менее чем из 6 символов.

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 7

4) В пароле должны присутствовать символы трех категорий из числа следующих четырех:

- прописные буквы английского алфавита от А до Z;
- строчные буквы английского алфавита от а до z;
- десятичные цифры (от 0 до 9);
- символы, не принадлежащие алфавитно-цифровому набору (например, символы: !, \$, #, % и т.д.)

Правила ввода пароля:

Во время ввода пароля необходимо исключить возможность его подсматривания посторонними лицами или техническими средствами (например, видеокамерами).

Правила хранения пароля:

- 1) Не рекомендуется записывать пароль на бумаге, в файлах, электронных записных книжках и других носителях информации.
- 2) Не рекомендуется сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

Правила изменения пароля:

Смену пароля рекомендуется проводить не реже одного раза в 3 месяца.

4.2 Выполнение требований законодательства РФ в области обработки и защиты персональных данных

Для выполнения требований законодательства РФ в области обработки и защиты персональных данных необходимо:

- скачать с закрытой части сайта www.fcii.ru и заполнить шаблоны документов;
- реализовать указанный в данных документах комплекс мер.

При выполнении требований эксплуатационной документации к СКЗИ, необходимо:

- вести Журнал учета СКЗИ (образец доступен на официальном сайте Фонда).
- дистрибутивы СКЗИ, Формуляры и ключевые документы должны быть учтены в Журнале учета СКЗИ;
- организовать хранение защищенных носителей и ключевых документов в соответствии с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 8

связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной Приказом ФАПСИ от 13.06.2011 №152 (далее – Инструкция) (опечатывание замочных скважин, индивидуальное хранилище для хранения ключевого носителя - сейф, опечатывающийся тубус и т.д.);

- осуществлять эксплуатацию средств СКЗИ в соответствии с эксплуатационной документацией;
- устанавливать только сертифицированные версии СКЗИ (оформляется актом установки и ввода в эксплуатацию, актом обучения и допуска пользователя к СКЗИ);
- при использовании КриптоПро CSP использовать усиленный режим использования ключей;
- выполнять требования разделов 2,3,4,5 Инструкции.



В соответствии с требованиями Федерального закона от 25 июля 2011 г. № 261-ФЗ "О внесении изменений в Федеральный закон "О персональных данных", программно-технические средства, применяемые для защиты персональных данных, должны пройти процедуру оценки соответствия (быть сертифицированы ФСТЭК и/или ФСБ России)

4.3 Антивирусная защита

Для соблюдения требований эксплуатационной документации СКЗИ и законодательства РФ в области обработки и защиты персональных данных необходимо применение антивирусного программного обеспечения, сертифицированного ФСБ России. Рекомендуется наличие сертификатов как ФСБ, так и ФСТЭК.

4.4 Защита информации от утечек

Защита от утечек конфиденциальной информации, в результате реализации угроз связанных с действиями внутреннего нарушителя, намеренных или случайных, имеющих легальные права доступа к конфиденциальным данным. Может быть реализована путем внедрения организационных мер (заключение соглашения о неразглашении конфиденциальной информации, ограничение прав доступа к конфиденциальной информации, учет носителей конфиденциальной информации и т.д.), либо путем применения специализированных систем предотвращения утечек информации (Data Leak Prevention System).

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 9

4.5 Межсетевое экранирование

Подсистема межсетевого экранирования предназначена для обеспечения защиты ПК пользователя ЕИС при подключении к сети Интернет.

Данная подсистема должна быть реализована путем применения программного и /или программно-аппаратного средства – межсетевой экран.



В силу того, что локальная база клиентского модуля ЕИС хранится только на персональных компьютерах нотариусов, настоятельно рекомендуется осуществлять регламентное (регулярное) резервное копирование данной базы.

4.6 Резервное копирование

4.6.1 Ручной режим

Для реализации резервного копирования штатными средствами операционной системы следует включить в создаваемый архив информационные ресурсы ЕИС (локальные базы данных и папки клиентского модуля ЕИС) и создавать точки восстановления в ОС по настраиваемому расписанию, не реже 1 раза в неделю, на отличный от основного жесткого диска носитель.

4.6.2 Автоматизированный режим

Для автоматизации резервного копирования информационных ресурсов, содержащих конфиденциальную информацию (локальные базы данных, файлов, папок и т.д.), рекомендуется дополнительно применять специализированные программные средства и/или программно-аппаратные комплексы. При их применении также следует создавать точки восстановления в ОС по настраиваемому расписанию.

5 АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

Для работы с ЕИС на стороне пользователя используется программно-аппаратный комплекс на основе персонального компьютера и следующих специализированных устройств:

- 1) Защищенный носитель ключевой информации - персональное средство аутентификации и защищенного хранения ключевой информации;
- 2) Планшет для рукописного ввода – графический планшет, оснащенный дисплеем, отображающим вводимую подпись в реальном времени.

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 10

При наличии в нотариальной конторе нескольких ПК, использующих общую базу данных, требования к системному блоку различаются в зависимости от количества подключений к локальному серверу СУБД.

Производительность ПК нотариуса ЕИС без внешних подключений определяется преимущественно производительностью жесткого диска, оптимально обеспечиваемой твердотельными дисками (SSD). Использование накопителей на магнитных дисках (HDD) рекомендуется только для резервных копий данных.

При подключении дополнительных рабочих мест к локальному серверу, для каждого подключения создается дополнительный процесс СУБД, поэтому целесообразно увеличение количества потоков процессора и объема памяти. Эффективная организация дополнительных рабочих мест может быть обеспечена при помощи виртуальных рабочих столов (VDI).

Таблица 2. Рекомендуемые характеристики оборудования

Компонент	Характеристика	Рекомендуемые значения	
		Минимальные	Оптимальные
Системный блок			
Общие требования			
Процессор	Архитектура	64-разрядная (x86-64)	
	Количество ядер	2	4
	Тактовая частота	2,4 ГГц	≥ 3,2 ГГц
	Примеры моделей		AMD Ryzen 3 3200G Intel Core i3-9100
Оперативная память	Объем	≥ 4 ГБ	16 ГБ
Видеоадаптер	Тип	Встроенный или дискретный	
	Поддержка интерфейса	DirectX 9	DirectX 11
	Объем видеопамяти	128 МБ (для дискретных адаптеров)	≥ 1 ГБ (для дискретных адаптеров)
	Примеры моделей		nVidia GT 710 Radeon R5 230
Системный жесткий диск	Технология		Твердотельный (SSD)
	Объем	≥ 240 ГБ	≥ 480 ГБ
	Интерфейс		M.2 PCI-Express
	Примеры моделей	Kingston A400 WD Green WDS240	HP SSD EX900 Transcend MTE110S
Контроллеры USB	Версия	USB 2.0	USB 3.0
	Количество	4	8
Хранилище резервных копий	Тип	Внешний жесткий диск	NAS-хранилище
	Объем дисков	≥ 1 ТБ	≥ 1 ТБ * 2
	Интерфейс	USB 3.0	Ethernet (RJ-45)

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 11

Компонент	Характеристика	Рекомендуемые значения	
		Минимальные	Оптимальные
Оптический привод	Тип	DVD-RW (Прим.: для передачи документов. Не используется ПО ЕИС.)	
Системный блок, выполняющий роль локального сервера СУБД ЕИС (дополнительные требования)			
От 1 до 4 клиентских подключений			
Процессор	Количество ядер	2	4
	Тактовая частота	2,4 ГГц	≥ 3,2 ГГц
Оперативная память	Объем	≥ 4 ГБ	16 ГБ
От 5 до 10 клиентских подключений			
Процессор	Количество ядер	2	≥ 4
	Количество потоков	4	≥ 6
	Тактовая частота	2,4 ГГц	≥ 3,2 ГГц
	Примеры моделей	AMD Ryzen 5 3400G Intel Core i5-9400	
Оперативная память	Объем	8 ГБ	≥ 16 ГБ
Жесткий диск с СУБД	Технология	Твердотельный (SSD)	
	Объем	≥ 480 ГБ	
Свыше 10 клиентских подключений			
Процессор	Количество ядер	4	≥ 6
	Количество потоков	8	≥ 12
	Тактовая частота	3,2 ГГц	≥ 3,6 ГГц
	Примеры моделей	AMD Ryzen 7 3700 Intel Core i7-9700	
Оперативная память	Объем	16 ГБ	32 ГБ
Жесткий диск с СУБД	Технология	Твердотельный (SSD)	
	Объем	≥ 480 ГБ	
	Интерфейс		M.2 PCI-Express
	Примеры моделей	HP SSD EX950 Transcend MTE220S	
Клиент, подключенный к СУБД на другом компьютере			
Процессор	Количество ядер	2	≥ 2
	Количество потоков		4
	Тактовая частота	2,4 ГГц	≥ 3,2 ГГц
	Примеры моделей	AMD Athlon 3000G Intel Pentium G5420	
Оперативная память	Объем	≥ 4 ГБ	≥ 8 ГБ
Жесткий диск	Объем	≥ 120 ГБ в зависимости от установленного ПО	
Виртуализированный клиент (Virtual desktop)			

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 12

Компонент	Характеристика	Рекомендуемые значения	
		Минимальные	Оптимальные
Процессор	Количество логических ядер	2	4
Оперативная память	Объем	4 ГБ	4-6 ГБ
Устройства ввода / вывода			
Монитор	Разрешение	≥ 1680x1050	≥ 1920x1080
	Количество цветов		16.7 млн.
	Диагональ		≥ 24”
Средство создания квалифицированной электронной подписи			
Защищённый ключевой носитель	Модели	eToken PRO Jacarta PRO SafeNet eToken	
Периферийные устройства			
Сканер	Тип	Планшетный	МФУ с автоматической подачей
	Интерфейс	USB 2.0	USB 2.0 + Ethernet
	Разрешение	≥ 600x600 т/д	≥ 600x600 т/д
	Формат файлов сканирования	tiff, jpeg	tiff, jpeg, pdf, doc
Принтер	Интерфейс	USB 2.0+	Ethernet (RJ-45)
	Разрешение для ч/б печати	≥ 600x600 т/д	≥ 600x600 т/д
	Скорость печати	7 стр/мин (ч/б А4)	35 стр/мин (ч/б А4)
	Технология печати	Лазерная	Лазерная
Планшет для создания ПЭП	Модели	Wacom STU-430	Wacom STU-540
Веб-камера	Интерфейс	USB 2.0+	USB 2.0+
	Разрешение	1280x720	1920x1080
	Частота кадров	30 к/с	60 к/с
	Микрофон	+	С шумоподавлением
	Примеры моделей	Logitech C310 Logitech C270	Logitech C925e Logitech C920
Канал передачи данных в сеть Интернет			
Основной	Тип		Выделенная линия
	Скорость	≥ 1 Мбит/с	≥ 10 Мбит/с
Резервный	Скорость		≥ 1 Мбит/с
Источник бесперебойного питания			
ИБП	Мощность	≥ 650 VA ≥ 200% максимальной фактической нагрузки	
	Время работы (автономной)	≥ 5 минут	

Приведенные в столбце «Оптимальные» характеристики определены с учетом состояния рынка оборудования на 2020 год, и рассчитаны на обеспечение комфортной работы в течение всего срока службы вновь

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 13

приобретаемого оборудования, с учетом ожидаемого развития ЕИС. Данные характеристики рекомендуется учитывать при приобретении нового оборудования.

Приведенные в столбце «Минимальные» характеристики необходимы для обеспечения штатной работы сервисов ЕИС.

6 ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Для работы с ЕИС на стороне пользователя необходимо общесистемное, прикладное и специализированное программное обеспечение, рекомендуемые типы и версии которого приведены в таблице 3.

Таблица 3. Рекомендуемое программное обеспечение

Вид ПО	Рекомендуемое ПО	
	Минимальное	Оптимальное
Общесистемное программное обеспечение		
Операционная система	Microsoft Windows 8.1 Professional	Microsoft Windows 10 64-разрядная
Прикладное программное обеспечение		
ПО клиентской части ЕИС	Клиентский модуль ЕИС, иное программное обеспечение согласно требованиям и рекомендациям ФНП	
Интернет-браузер	Google Chrome последней версии, Спутник	
Расширения интернет-браузера	CryptoPro Extension for CAdES Browser Plug-in, КриптоПро ЭЦП Browser plug-in.	
Специализированное программное обеспечение		
Средства формирования и проверки ЭП	СКЗИ КриптоПро CSP версии 4.0 R3, 4.0 R4	СКЗИ КриптоПро CSP версии 4.0 R4
Информационная безопасность		
Разграничение и контроль доступа	Штатные средства ОС (защита учетной записи паролем)	Штатные средства ОС + специализированные СЗИ
Средства обеспечения целостности и доступности	Резервное копирование средствами ОС и клиентского модуля ЕИС	Специализированное ПО и ПАК + резервное копирование средствами ОС и клиента ЕИС
Межсетевой экран	Штатные средства ОС	Специализированные межсетевые экраны
Антивирусное ПО	Сертифицированное ФСБ России	Сертифицированное ФСТЭК России и ФСБ России
Средства защиты информации от утечек	Организационные меры	Специализированное ПО для противодействия утечкам конфиденциальной информации
Криптографическая защита	Шифрование файлов, папок, и локальных баз данных клиента ЕИС, с обязательным наличием средств восстановления ключей шифрования.	

Наименование:	Рекомендации по оборудованию и программному обеспечению для нотариальной конторы	
Название документа:	Рекомендации для пользователей	Стр. 14



Важными условиями стабильной и корректной работы клиентской части ЕИС и системы криптографической защиты информации КристоПРО CSP являются:

- 1. Отсутствие на ПК пользователя ЕИС нелицензионного программного обеспечения.*
- 2. Выполнение требований эксплуатационной документации к СКЗИ и СЗИ.*
- 3. Выполнение требований законодательства РФ в области обработки и защиты персональных данных.*