|  |  |
| --- | --- |
|  | Приложение 3 к Регламенту подключения к системе межведомственного электронного документооборота в Донецкой Народной Республике, а также работы с электронными сообщениями, электронными документами (копиями электронных документов) и (или) электронными копиями документов в системе межведомственного электронного документооборота в Донецкой Народной Республике(подпункт «в» пункта 4.2) |

**ТРЕБОВАНИЯ**

**к автоматизированным рабочим местам пользователей государственной информационной системы электронного делопроизводства и документооборота в Донецкой Народной Республике**

1. **Системные требования** **рабочего места**
   1. Системные требования к оборудованию автоматизированного рабочего места пользователя государственной информационной системы электронного делопроизводства и документооборота в Донецкой Народной Республике (далее – СЭДД):

процессор: от 2 ядер по 2,4 ГГц;

оперативная память: 2 ГБ и выше;

свободное место на жестком диске: не менее 1 Гб;

соединение с сетью «Интернет» не менее 6 Мб/с.;

минимальное разрешение экрана: 1024 x 768.

* 1. Для использования всех функциональных возможностей СЭДД на рабочей станции должны быть установлены:

лицензионная операционная система, включенная в Единый реестр российских программ для электронных вычислительных машин и баз данных,  
с действующей технической поддержкой;

пакет лицензионных офисных приложений, включенных в Единый реестр российских программ для электронных вычислительных машин и баз данных,  
с действующей технической поддержкой;

браузер для отображения веб-страниц, поддерживающий Transport Layer Security (TLS v. 1.0/1.2, RFC 5246), с использованием российских криптографических стандартов;

программное обеспечение для использования опции сканирования и для работы подсистемы «Поточное сканирование».

1. **Требования по разграничению доступа**
   1. Пользователи допускаются к работе с ресурсами СЭДД на основании приказа руководителя соответствующего участника межведомственного электронного документооборота в Донецкой Народной Республике (далее – участник) после прохождения обучения по использованию СЭДД и успешного выполнения тестового задания, подготовленного оператором системы межведомственного электронного документооборота в Донецкой Народной Республике (далее – оператор). Примерное тестовое задание оператор размещает на своем официальном сайте. Результаты выполнения тестового задания фиксируются в сертификате, выдаваемом оператором пользователю.
   2. К работе в СЭДД допускаются пользователи, подписавшие обязательство о неразглашении конфиденциальной информации.
   3. Пароль учетной записи пользователя должен отвечать следующим требованиям:
2. уникальность: пароль не должен совпадать частично или полностью с уже использованными паролями данного пользователя;
3. конфиденциальность: пароль учетной записи должен знать только пользователь. Не допускается передача пароля третьим лицам ни при каких условиях.
   1. В целях организации упорядоченного и избирательного доступа к автоматизированному рабочему месту программное обеспечение, установленное на нем, должно обеспечивать выполнение следующих требований:
4. осуществляется автоматическая блокировка автоматизированного рабочего места при отсутствии активности пользователя более 5 (пяти) минут, а также по запросу пользователя;
5. осуществляться автоматическая блокировка автоматизированного рабочего места в случае 5 (пяти) неуспешных попыток входа в информационную систему;
6. гостевая учетная запись автоматизированного рабочего места должна быть заблокирована;
7. реализован доступ пользователя к СЭДД только под учетной записью с ограниченными правами. Запрещается работа с системой в привилегированном режиме (авторизация в системе с учетной записью, имеющей права администратора);
8. при наличии в информационной системе участника доменной структуры все локальные учетные записи автоматизированного рабочего места должны быть заблокированы;
9. доступ пользователей к автоматизированному рабочему месту должен осуществляться в строгом соответствии с матрицей доступа.
   1. Технические средства автоматизированного рабочего места должны находиться в условиях, исключающих несанкционированный доступ. Случайный просмотр экрана монитора автоматизированного рабочего места посторонними людьми должен быть исключен.
   2. Помещение, в котором находятся технические средства, должно быть оборудовано охранно-пожарной сигнализацией и в период отсутствия сотрудников в помещении сдаваться под охрану.
10. **Требования к программно-техническому обеспечению**
    1. Запрещается использование беспроводной клавиатуры и (или) мыши, а также радиоинтерфейсов передачи данных (Wi-Fi, WiMAX, Bluetooth и др.).
    2. Запрещено оборудовать автоматизированное рабочее место дополнительными сетевыми адаптерами для одновременного подключения к другим сетям.
    3. Встроенные механизмы безопасности операционной системы не должны быть отключены.
    4. На автоматизированном рабочем месте должна быть установлена только одна операционная система.
    5. В настройках BIOS автоматизированного рабочего места должен быть установлен запрет на загрузку с внешних носителей, а также установлен пароль на вход в BIOS.
    6. На автоматизированном рабочем месте должны отсутствовать программы развлекательного характера (игры, гороскопы, программы – розыгрыши и т.д.) и другое программное обеспечение, не связанное непосредственно с исполнением служебных обязанностей, а также средства разработки и отладки программ (кроме средств разработки, встроенных в прикладное программное обеспечение, выборочное удаление которых не предусмотрено разработчиком прикладного программного обеспечения).
    7. Подключаемые к СЭДД рабочие места пользователей необходимо оснастить сертифицированными средствами защиты информации:
11. системой защиты от несанкционированного доступа и раскрытия информации ограниченного доступа;
12. программным комплексом, выполняющим на рабочем месте функции VPN-клиента, персонального экрана, клиента защищенной почтовой системы,  
    а также криптопровайдера для прикладных программ, использующих функции подписи и шифрования;
13. электронный ключ eTokenPROJava с USB интерфейсом.
    1. Подключаемые к СЭДД рабочие места пользователей необходимо оснастить лицензионными средствами антивирусной защиты, включенными в Единый реестр российских программ для электронных вычислительных машин и баз данных, с действующей технической поддержкой.