АДМИНИСТРАЦИЯ БОЛЬШЕСОЛДАТСКОГО РАЙОНА КУРСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

от 01.08.2023 № 143-р

Курская область, с. Большое Солдатское

Об утверждении требований к оснащению автоматизированных рабочих мест Администрации Большесолдатского района Курской области и порядка их использования

В целях регламентирования мероприятий по оснащению и распределению основных и вспомогательных технических средств, программного обеспечения и обеспечения безопасности информационных систем:

1. Утвердить прилагаемые требования к оснащению автоматизированных рабочих мест Администрации Большесолдатского района Курской области и порядок их использования.
2. Консультанту-программисту по защите информации Администрации Большесолдатского района Курской области, Шамаеву Сергею Александровичу, обеспечить опубликование постановления на официальном сайте муниципального района «Большесолдатский район» Курской области в информационно-телекоммуникационной сети «Интернет».
3. Контроль за исполнением настоящего распоряжения возложить на Первого заместителя Главы Администрации Большесолдатского района Курской области Чупикова В. А..
4. Распоряжение вступает в силу со дня опубликования.

Глава Большесолдатского района
Курской области В. П. Зайцев

Утверждены
Распоряжением Администрации
Большесолдатского района
Курской области
От 01.08.2023 №143-р

Требования к оснащению автоматизированных рабочих Администрации Большесолдатского района Курской области и порядок их использования.

1. Сокращения и термины

1.1. ЕИКС - сеть передачи данных единой информационной коммуникационной среды Курской области.

1.2. АРМ - автоматизированное рабочее место (совокупность средств вычислительной техники и программного обеспечения) сотрудников Администрации Большесолдатского района Курской области.

1.3. Пользователь АРМ – сотрудник Администрации Большесолдатского района Курской области, осуществляющий на АРМ служебные функции.

1.4. СВТ - средства вычислительной техники.

1.5. ПО - лицензионное программное обеспечение, закупленное в рамках обеспечения рабочего процесса в Администрации Большесолдатского района Курской области.

2. Общие положения

2.1. Требования и порядок использования АРМ работников Администрации Большесолдатского района Курской области разработаны с целью регламентирования мероприятий по оснащению и распределению основных и вспомогательных технических средств, ПО в Администрации Большесолдатского района Курской области и распространяются на АРМ, на которых обрабатывается общедоступная информация.

2.2. Под основными и вспомогательными техническими средствами понимаются СВТ, указанные в приложениях NN 1 - 2 к настоящим требованиям.

2.3. СВТ и ПО предназначены для:

обеспечения функциональной деятельности Администрации Большесолдатского района Курской области путем автоматизации информационных процессов;

интеграции и подключения АРМ сотрудников к централизованным вычислительным сервисам и мощностям;

обеспечения непрерывного и оперативного обмена информацией между ОМС;

организации эффективного межведомственного электронного документооборота;

обеспечения защиты информации, обрабатываемой на АРМ.

2.4. СВТ должны обеспечивать:

высокую степень надежности и отказоустойчивости информационной системы;

возможность гибкого наращивания и реконфигурации при минимальных затратах в случае перехода на новые информационные технологии;

полную совместимость аппаратной части комплекса и ПО.

2.5. Данный документ предназначен для использования в качестве основного правового документа при планировании оснащения и распределении СВТ и ПО в

Администрации Большесолдатского района Курской области, подготовке конкурсных требований на поставку СВТ и ПО, а также при эксплуатации имеющихся АРМ.

2.6. Настоящие требования ориентированы на применение в течение 3 лет, периодически уточняются и обновляются с учетом развития информационных технологий.

3. Общие требования АРМ

3.1. К вновь приобретаемым СВТ и ПО предъявляются следующие требования:

СВТ и ПО должны иметь сертификаты соответствия, действующие на территории Российской Федерации;

ПО (в том числе операционные системы) должно быть лицензионным (проприетарным или свободно распространяемым) и включено в единый реестр российских программ для электронных вычислительных машин и баз данных (за исключением случаев невозможности соблюдения запрета на допуск программного обеспечения, происходящего из иностранных государств).

3.2. Гарантийные обязательства:

гарантийный срок на поставляемое СВТ должен составлять не менее 1 года;

гарантийное и послегарантийное техническое обслуживание поставляемого оборудования должно проводиться силами сертифицированных центров поставщика или производителя.

Минимальные технические параметры СВТ указаны в приложениях NN 1 - 2 к настоящим требованиям. Данные параметры должны применяться к вновь приобретаемым АРМ.

В случае если существующие АРМ не соответствуют вышеуказанным требованиям, то рекомендуется по мере возможности привести их в соответствие с настоящими требованиями.

4. Техническое обслуживание АРМ

4.1. В Администрации Большесолдатского района техническое обслуживание возлагается на главного специалиста – эксперта отдела организационной работы (далее - специалист по информационно-программному обеспечению).

5. Порядок установки и сопровождения ПО в Администрации Большесолдатского района Курской области

5.1. Установка и сопровождение типового ПО.

5.1.1. Пользователь АРМ направляет заявку, содержащую информацию, перечисленную в пункте 7.2 настоящих требований, отдел по информационно-программному обеспечению для проведения процедуры установки типового ПО.

5.1.2. В случае возникновения сбоя в работе типового ПО пользователь АРМ направляет заявку, содержащую информацию, перечисленную в пункте 7.2 настоящих требований, в отдел по информационно-программному обеспечению с описанием причин и действий, после которых ПО прекратило функционирование.

5.2. Установка специализированного ПО.

5.2.1. Для установки данного ПО направляется письменный запрос Главе Администрации Большесолдатского района с описанием необходимого ПО.

Главе Администрации Большесолдатского района в течение 10 рабочих дней со дня поступления запроса принимает решение об использовании данного ПО и в случае

положительного решения дает указание отделу по информационно-программному обеспечению о проведении процедуры установки ПО.

5.2.2. В случае неработоспособности специализированного ПО пользователь АРМ направляет заявку, содержащую информацию, перечисленную в пункте 7.2 настоящих требований, в отдел по информационно-программному обеспечению с описанием причин и действий, после которых ПО прекратило функционирование.

6. Порядок использования ПО

6.1. Пользователь АРМ имеет право использовать предоставленное ему ПО для выполнения своих служебных обязанностей.

6.2. Пользователь АРМ должен обладать соответствующими знаниями (квалификацией) и опытом работы с установленным на его АРМ ПО. При отсутствии необходимых знаний и навыков работы пользователь АРМ должен в обязательном порядке пройти обучение.

6.3. Пользователь АРМ должен:

своевременно выполнять мероприятия по защите АРМ от вредоносного программного обеспечения;

самостоятельно выполнять копирование и архивирование информации, размещенной на АРМ, и нести личную ответственность в случае ее хищения, искажения или уничтожения.

6.4. Пользователю АРМ запрещается:

использовать предоставленное ПО в неслужебных целях, производить действия, приводящие к нарушению работоспособности отдельного ПО и всего АРМ в целом;

производить без разрешения Управляющего делами Администрации Большесолдатского района перемещение, копирование, удаление или передачу другим лицам предоставленного ему ПО;

производить удаление ПО;

изменять настройки и конфигурацию системного ПО;

самостоятельно производить установку типового, специализированного ПО или программного обеспечения, приобретенного или полученного в частном порядке, в том числе с нарушением лицензионных соглашений.

6.5. При выявлении фактов нарушений требований, перечисленных в пункте 6.4 настоящих требований, отделом по информационно-программному обеспечению составляется акт о выявленных нарушениях (порче) при пользовании АРМ.

7. Организация работ по сопровождению ПО

7.1. Работы по сопровождению ПО осуществляются соответственно силами специалиста по информационно-программному обеспечению

7.2. При обращении к специалисту по информационно-программному обеспечению пользователь АРМ должен сообщить следующую информацию (в заявке):

наименование структурного подразделения;

номер кабинета;

инвентарный номер системного блока АРМ;

фамилия, имя, отчество;

должность;

контактные данные;

причина обращения.

7.3. Специалист по информационно-программному обеспечению выполняет следующие работы:

выявление и устранение типовых нарушений, указанных в приложении N 3 к настоящим требованиям;

ведение паспортов АРМ согласно приложению N 4 к настоящим требованиям;

установка типового и специализированного ПО;

настройка системного ПО;

мероприятия по защите информации;

проверка работоспособности ПО;

устранение сбоев и неисправностей ПО (если данное представляется возможным);

проверка перечня установленных программных продуктов, а также наличие программных продуктов или информации, не относящейся к служебной деятельности пользователя АРМ.

7.4. В обязанности специалиста по информационно-программному обеспечению не входит:

настройка пользовательского интерфейса ПО;

установка и настройка лицензионного программного обеспечения и свободного программного обеспечения, приобретенного или полученного в частном порядке;

установка и сопровождение программных продуктов с нарушением лицензионных соглашений (нелицензионное программное обеспечение);

обучение пользователя АРМ работе с установленными на АРМ программными продуктами.

8. Парольная политика

8.1. Минимальные требования к сложности пароля:

Пароль не должен содержать имя учетной записи пользователя или какую-либо его часть или включать в себя легко вычисляемые сочетания символов (имена, фамилии и т.д.), а также общепринятые сокращения (LAN, USER и т.п.).

Пароль должен состоять не менее чем из 8 (восьми) символов.

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

прописные буквы английского алфавита от "A" до "Z";

строчные буквы английского алфавита от "a" до "z";

десятичные цифры (от 0 до 9);

неалфавитные символы (например, !, $, #, %).

В целях обеспечения информационной безопасности и противодействия попыткам подбора символы вводимого пароля не должны отображаться на экране в явном виде.

8.2. Порядок ввода и хранения пароля:

Непосредственно перед вводом пароля для предотвращения возможности неверного ввода пользователь должен убедиться в правильности языка ввода (раскладки клавиатуры), проверить, не является ли активной клавиша CAPSLOCK (если это необходимо), а также проконтролировать расположение клавиатуры (клавиатура должна располагаться таким образом, чтобы исключить возможность увидеть набираемый текст посторонними).

Не следует использовать один и тот же пароль для доступа к учетным записям и к другим ресурсам. Не рекомендуется использовать:

"домашние" пароли при работе со служебными ресурсами;

один пароль для доступа к двум и более ресурсам.

Пользователю запрещается нарушать конфиденциальность авторизационных данных своего АРМ, в том числе:

сообщать третьим лицам свой пароль по телефону;

передавать свой пароль по электронной почте;

произносить вслух свой пароль;

указывать свой пароль в анкетах или опросниках;

хранить пароль в общедоступном месте, в том числе в виде файла на компьютере и иных носителях информации.

Запрещается создавать подсказки на пароль (например, "мой день рождения").

Запрещается использовать функцию "Запомнить пароль".

8.3. Удаление/отключение учетной записи пользователя или смена пароля.

Кадровое подразделение Администрации Большесолдатского района должно известить специалиста по информационно-программному обеспечению в течение 1-го рабочего дня после увольнения сотрудника или перевода его в другое структурное подразделение о данном факте.

При необходимости работы на одном АРМ двух или более сотрудников Администрации Большесолдатского района для каждого сотрудника должна создаваться собственная учетная запись с правами пользователя.

9. Организация электронного взаимодействия с использованием электронной почты в Администрации Большесолдатского района Курской области

9.1. В соответствии с приказом Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю от 31 августа 2010 г. N 416/489 "Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования" информационные системы общего пользования должны обеспечивать:

сохранность и неизменность обрабатываемой информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения;

беспрепятственный доступ пользователей к информации, содержащейся в информационной системе общего пользования;

защиту от действий пользователей в отношении информации, не предусмотренных правилами пользования информационной системой общего пользования, приводящих, в том числе, к уничтожению, модификации и блокированию информации;

поддержание целостности и доступности информации;

предупреждение возможных неблагоприятных последствий нарушения порядка доступа к информации;

своевременное обнаружение фактов неправомерных действий в отношении информации;

возможность оперативного восстановления информации, модифицированной или уничтоженной вследствие неправомерных действий.

9.2. Электронные почтовые ящики Администрации Большесолдатского района должны использоваться только в служебных целях. Запрещается:

рассылка личных почтовых сообщений;

спама (нежелательные электронные письма, как правило, рекламного характера);

вложений с вирусами;

сообщений неэтичного или противозаконного характера.

9.3. Защита информации, содержащейся в информационных системах общего пользования, достигается путем исключения неправомерных действий в отношении указанной информации. Использование иностранных почтовых серверов (@gmail.com, @hotmail.com и т.п.), а также пересылка служебной информации посредством стороннего программного обеспечения (социальные сети, Skype и т.п.) категорически запрещена.

В связи с отсутствием данных об уровне защищенности информации при использовании почтовых серверов общего пользования, таких как @rambler.ru, @yandex.ru, @mail.ru и т.п., для взаимодействия органов исполнительной власти Курской области посредством электронной почты необходимо обеспечить переход от использования сторонних почтовых доменов к работе с применением почтовых серверов Администрации Курской области (@rkursk.ru, @rkursk.eiks) либо собственных защищенных почтовых серверов ОИВ.

9.4. Порядок организации работы с использованием электронной почты.

Для ведения деловой переписки посредством электронной почты ОИВ обязаны использовать (срок перехода - до 2018 года):

почтовый сервер Администрации Курской области (@rkursk.ru);

собственные защищенные почтовые серверы ОИВ;

почтовый сервер ГУП Курской области "Информационный Центр "Регион-Курск".

В случае отсутствия возможности применения почтового сервера Администрации Курской области необходимо направить письмо в адрес Комитета с указанием причины.

Для осуществления общения между ОИВ необходимо использовать:

внутренний почтовый сервер (@rkursk.eiks), расположенный в ЕИКС;

собственные почтовые серверы ОИВ, имеющие внутренние IP-адреса ЕИСК, которые внесены в DNS ЕИКС;

внутренний почтовый сервер ГУП Курской области "Информационный Центр "Регион-Курск".

В каждом ОИВ должен быть создан и актуализирован список почтовых адресов, принадлежащих специалистам ОИВ.

В целях актуализации базы данных адресов электронной почты необходимо предоставлять информацию обо всех изменениях адресации в Комитет не реже двух раз в год (в срок до 1 апреля и до 1 октября текущего года).

9.5. Процедура получения почтовых ящиков на почтовых серверах Администрации Курской области, а также инструкция по настройке почтового клиента содержатся в приложениях NN 5 - 6 к настоящим требованиям.

9.6. Рекомендации по защите электронной почты.

На всех персональных компьютерах, оснащенных почтовыми клиентами, должно быть установлено сертифицированное антивирусное программное обеспечение.

Перед работой с e-mail необходимо убедиться, что антивирусные базы программных средств защиты актуальны и включена функция защиты почтового клиента.

Необходимо использовать только лицензионные почтовые клиенты.

В соответствии с разделом 9 настоящих требований для почтовых ящиков нужно устанавливать парольную защиту.

При разборе полученной почты необходимо обращать особое внимание на файлы, вложенные в письма. Файлы, имеющие двойное расширение типа EXE, COM, BAT, PIF, DLL, BIN, VBS (для маскировки между ними могут стоять пробелы), могут представлять опасность для АРМ или ЕИКС (например: Komitet.jpg.vbs). Первое расширение таких вложений создает ложное представление о безобидности вложенного файла, но последнее явно указывает, что вложение содержит в себе исполняемый вредоносный файл.

Не рекомендовано:

переходить по гиперссылкам, содержащимся в электронных письмах, так как они могут перенаправлять на ресурсы, содержащие вредоносное программное обеспечение;

отправлять письма с вложенными файлами, превышающие общий объем 10 Mb.

Рекомендуется выполнять резервное копирование адресной книги, входящих и исходящих сообщений.

9.7. Порядок работы с электронной почтой.

При отправке важных писем в сообщении должна указываться необходимость подтверждения получения письма адресатом.

Перед отправлением сообщения необходимо проводить проверку правописания и грамматики текста сообщения. Тексты большого объема желательно отправлять в виде вложения.

Электронные письма обязательно должны быть подписаны лицом, производившим отправку корреспонденции. Необходимо настроить почтовый клиент для автоматической вставки подписи в почтовые отправления. Подпись должна содержать: имя, отчество и фамилию отправителя, должность, название ОИВ, контактного телефона отправителя.

При получении спама необходимо сразу удалить такие письма, не открывая вложение (желательно провести добавление отправителя в список заблокированных отправителей).

Не рекомендуется удалять входящие и исходящие письма в течение года. В дальнейшем, во избежание переполнения электронного ящика, старые неактуальные письма можно удалить по согласованию с руководителем.

Желательно сформировать структуру папок для упорядочения входящих сообщений. Все передаваемые по электронной почте вложения (файлы) должны быть предварительно проверены антивирусными средствами.

Передаваемые с помощью электронной почты официальные документы должны иметь соответствующие реквизиты (исходящий регистрационный номер, номер и дату приказа, распоряжения и т.п.). В тексте сообщения необходимо обязательно указывать реквизиты и название пересылаемого во вложении официального документа. Передаваемая и принимаемая в адрес Администрации Большесолдатского района официальная электронная корреспонденция регистрируется в соответствии с правилами делопроизводства.

10. Обновление программного обеспечения

11.1. В целях повышения производительности, обеспечения совместимости со вновь появившимся оборудованием, а также для устранения уязвимостей безопасности существующих информационных систем необходимо проводить своевременное обновление программного обеспечения в соответствии с порядком, указанным в приложении N 7 к настоящим требованиям.

11. Резервное копирование (восстановление) информации

12.1. Примерный порядок резервного копирования рабочей информации.

Регулярность создания резервных копий рабочей информации должна быть достаточной для продолжения нормальной работы Администрации Большесолдатского района, в случае нарушения целостности или доступности рабочей информации, но не реже одного раза в день для ежедневно изменяющихся данных и одного раза в неделю для периодически изменяющихся данных. Архивирование резервных копий на электронные носители (внешние дисковые хранилища и т.п.) должно осуществляться регулярно, но не реже одного раза в месяц.

Все резервные копии должны быть размещены в отдельных каталогах, название которых отражает дату последнего изменения рабочей информации и ее краткое описание (например, 01-04-2012_Buhgalteria).

Вся рабочая информация, хранящаяся на аппаратных ресурсах Администрации Большесолдатского района и регулярно копируемая на электронные носители, должна быть доступна для дальнейшего восстановления.

Как минимум одна резервная копия рабочей информации должна храниться на электронном носителе.

12.2. Примерный порядок хранения резервных копий.

Для хранения резервных копий на электронных носителях должны выбираться такие электронные носители, характеристики которых не изменяются в течение предполагаемого времени хранения резервных копий.

Хранение резервных копий рабочей информации на электронных носителях должно осуществляться с организацией контролируемого доступа к данным носителям, их защитой от воздействия окружающей среды.

12.3. Должен производиться периодический контроль исполнения процедуры резервного копирования (восстановления) информации.

12. Проведение мероприятий по защите информации

Основным средством предотвращения вирусного заражения АРМ из файлов документов (информации) и исполняемых файлов (программ) на сменных носителях и вложений в сообщениях электронной почты является антивирусное ПО, сертифицированное ФСТЭК России, установленное на АРМ.

12.1. Специалист по информационно-программному обеспечению осуществляет:

установку и настройку антивирусного ПО, в том числе настройку обновления антивирусного ПО и антивирусных баз;

администрирование и настройку серверной части антивирусного ПО (в случае наличия);

отключение АРМ от локально-вычислительной сети в случае выявления фактов заражения АРМ вредоносным программным обеспечением;

восстановление работоспособности АРМ после вирусного заражения;

мониторинг потенциальных угроз и реальных случаев заражения АРМ;

разработку инструкций и методологических рекомендаций пользователю АРМ по применению программно-технических средств антивирусной защиты;

проведение профилактических работ.

12.2. Меры по предотвращению вирусного заражения из файлов документов, расположенных на сменных носителях.

13.2.1. Для предотвращения вирусного заражения из файлов документов, полученных на сменных носителях, пользователю АРМ необходимо:

а) проводить с помощью антивирусного ПО проверку всех файлов, расположенных на получаемом им сменном носителе, до начала работы с этими файлами;

б) при обнаружении антивирусным ПО признаков вирусного заражения файлов самостоятельно, посредством антивирусного ПО, провести мероприятия по обезвреживанию вредоносного файла или программного обеспечения. В случае невозможности самостоятельного обезвреживания немедленно прекратить работу с данным сменным носителем;

в) о факте обнаружения на носителе зараженного файла сообщить специалисту по информационно-программному обеспечению и передать зараженный носитель.

12.2.2. Специалист по информационно-программному обеспечению при получении от пользователя АРМ зараженного внешнего носителя проводит анализ заражения и принимает все возможные меры для устранения заражения. Если заражение удалось ликвидировать, носитель возвращается пользователю АРМ. В ином случае отдел по информационно-программному обеспечению обязан передать зараженные файлы в компанию разработчика антивирусного ПО, а сам носитель запретить использовать до полного решения данной проблемы.

12.2.3. Контроль за исполнением требований подпункта 12.2.1 пункта 12.2 настоящих требований возлагается на отдел по информационно-программному обеспечению.

12.3. Меры по предотвращению вирусного заражения из файлов документов, поступивших как вложения в сообщения электронной почты.

13.3.1. Для предотвращения вирусного заражения из файлов документов, поступивших как вложения в сообщения электронной почты, пользователь АРМ обязан:

а) перед началом работы с вложенным файлом проверить его антивирусным ПО;

б) при обнаружении антивирусным ПО признаков вирусного заражения файлов самостоятельно, посредством антивирусного ПО, провести мероприятия по обезвреживанию вредоносного файла. В случае невозможности самостоятельного обезвреживания немедленно прекратить работу с данным файлом;

в) о факте обнаружения зараженного файла сообщить в отдел по информационно-программному обеспечению.

12.3.2. Специалист по информационно-программному обеспечению при поступлении от пользователя АРМ сообщения о зараженных файлах проводит анализ заражения и принимает все возможные меры для устранения заражения. Если заражение не удалось ликвидировать, специалист по информационно-программному обеспечению обязан передать зараженные файлы в компанию разработчика антивирусного ПО, а сам файл ликвидируется.

12.3.3. Контроль за исполнением требований подпункта 12.3.1 пункта 12.3 настоящих требований возлагается на специалиста по информационно-программному обеспечению.

12.4. Профилактические меры по предотвращению заражения вирусами АРМ.

12.4.1. В целях профилактики заражения АРМ вирусами пользователю АРМ необходимо:

12.4.1.1. Ежедневно перед началом работы проверять актуальность антивирусных баз и антивирусного ПО. В случае выявления фактов неактуальности антивирусных баз или антивирусного ПО незамедлительно сообщать специалисту по информационно-программному обеспечению.

12.4.1.2. Ежедневно перед началом работы проводить "быструю" проверку АРМ средствами установленного антивирусного ПО.

12.4.1.3. Один раз в месяц проводить "полную" проверку АРМ средствами антивирусного ПО.

12.4.1.4. При обнаружении признаков заражения файлов прекратить работу на АРМ, сообщить о факте заражения специалисту по информационно-программному обеспечению. Продолжение работы на данном АРМ допускается только по факту проверки и устранения причины заражения в случае выявления таковой сотрудником отдела по информационно-программному обеспечению независимо от срочности выполняемых на АРМ работ.

12.4.2. Специалист по информационно-программному обеспечению проводит анализ заражения АРМ и принимает все возможные меры для устранения заражения. Если заражение удалось ликвидировать, АРМ возвращается пользователю и дается разрешение для работы. В ином случае специалист по информационно-программному обеспечению обязан передать зараженные файлы в компанию разработчика антивирусного ПО, а АРМ запретить для использования до полного решения проблемы.

12.4.3. Контроль за исполнением требований подпункта 12.4.1 пункта 12.4 настоящих требований возлагается на специалиста по информационно-программному обеспечению.

12.5. Обновление антивирусного ПО:

В целях совершенствования системы антивирусной защиты специалист по информационно-программному обеспечению осуществляет:

своевременное обновление антивирусного ПО, установку необходимых дополнений, расширяющих число обнаруживаемых вирусов;

ведение систематизированного учета фактов и видов вирусного заражения файлов АРМ, а также взаимодействие с поставщиком (компанией - разработчиком) антивирусного ПО при подозрениях на наличие новых вирусов, не обнаруженных текущей версией антивирусного ПО.

Приложение N 1
к требованиям к оснащению
автоматизированных рабочих мест
Администрации Большесолдатского района
Курской области и
порядку их использования

МИНИМАЛЬНЫЕ ТЕХНИЧЕСКИЕ ПАРАМЕТРЫ
ОСНОВНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Технический параметр	Рабочая станция	Ноутбук
Процессор		
Частота работы процессора, ГГц	3	3
Количество ядер	2	2
Оперативная память		
Объем оперативной памяти, Гб	4	4
Видео		
Объем видеопамяти, Мб	1024	1024
Устройства хранения данных		
Тип оптического привода	DVD RW	DVD RW
Объем жесткого диска HDD, Гб	500	300
Объем жесткого диска SSD, Гб	500	-
Внешние проводные интерфейсы		
Пропускная способность сетевого интерфейса, Гбит/сек	1	1
USB, шт.	6	3
Звуковой интерфейс	наличие	наличие
Беспроводная связь		
WiFi	-	наличие
Звуковые, видеоустройства		
Колонки	опционально	опционально
Web-камера со встроенным микрофоном (разрешение)	опционально	наличие (1280 x 720)

Монитор (экран)		
Размер	22"	14"
Клавиатура, манипулятор "мышь"		
Цифровой блок на клавиатуре	наличие	опционально
Манипулятор "мышь"	наличие	наличие
Интерфейс клавиатуры	USB	-
Интерфейс манипулятора "мышь"	USB	USB
Блок питания		
форм-фактор ATX, Вт	500	-
форм-фактор SFX, Вт	180	-
Дополнительно		
Время работы в автономном режиме, час	-	3

Приложение N 2
к требованиям к оснащению
автоматизированных рабочих мест
Администрации Большесолдатского района
Курской области и
порядку их использования

МИНИМАЛЬНЫЕ ТЕХНИЧЕСКИЕ ПАРАМЕТРЫ ВСПОМОГАТЕЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ

Принтер

Тип печати	Черно-белая
Формат бумаги	А4
Автоматическая двусторонняя печать	наличие
Скорость печати, страниц в минуту	20
Время выхода первого отпечатка, секунд	10
Ресурс картриджа, страниц 5%	2000
USB	наличие

Сканер

Тип	планшетный/протяжный
Формат бумаги	А4
Скорость сканирования, страниц в минуту	15
USB	наличие

Многофункциональное устройство

Тип печати	Черно-белая
Формат бумаги	А4
Автоматическая двусторонняя печать	наличие
Время выхода первого отпечатка, секунд	10
Скорость печати, страниц в минуту	20
Скорость сканирования, страниц в минуту	15
Скорость копирования, страниц в минуту	20
Ресурс картриджа, страниц 5%	2000
USB	наличие

Приложение N 3
к требованиям к оснащению
автоматизированных рабочих мест
Администрации Большесолдатского района
Курской области и
порядку их использования

ТИПОВЫЕ НАРУШЕНИЯ И МЕРЫ ПО ИХ УСТРАНЕНИЮ

N п/п	Типовые нарушения, выявленные в ходе проверки	Меры по устранению типовых нарушений		
			Исполнитель	Срок
1.	Отсутствие пароля или использование пароля, не соответствующего парольной политике	Установить пароль для входа в операционную систему под учетными записями пользователей и администратора АРМ, соответствующий парольной политике	Специалист по информационно-программному обеспечению	В течение недели со дня выявления нарушения
2.	Работа пользователей на АРМ посредством учетной записи, обладающей правами администратора	Наделить всех пользователей ограниченными правами, необходимыми для исполнения служебной деятельности	Специалист по информационно-программному обеспечению	В течение недели со дня выявления нарушения
3.	Работа пользователя на АРМ посредством стандартных учетных записей	Отключить или ограничить доступ к ОС посредством стандартных учетных записей ОС	Специалист по информационно-программному обеспечению	В течение недели со дня выявления нарушения
4.	Наличие на АРМ вредоносного ПО	Проводить периодическую полную проверку АРМ посредством антивирусного ПО	Специалист по информационно-программному обеспечению	В течение рабочего дня со дня выявления
5.	Использование несертифицированных средств защиты информации (антивирусное ПО) или их полное отсутствие. Отсутствие обновления антивирусного ПО и антивирусных баз данных	Установить сертифицированные средства защиты информации (антивирусное ПО). Государственный реестр сертифицированных средств защиты	Специалист по информационно-программному обеспечению	В течение недели после закупки

		информации размещен на сайте ФСТЭК России (http://fstec.ru). Настроить ежедневное обновление антивирусного ПО и антивирусных баз данных, а также осуществлять контроль за данным обновлением. Установить ограничения на выгрузку (отключение/удаление) антивирусного ПО		
6.	Использование неслужебных устройств (мобильные телефоны, фотоаппараты, "домашние" (неучтенные) накопители данных, ноутбуки, планшеты). Запрещается подключать к локальной сети и служебным АРМ	Провести инвентаризацию USB-устройств, запретить установку драйверов для неучтенных USB-устройств, провести инструктаж пользователей АРМ об использовании в служебной деятельности только учтенных USB-устройств	Специалист по информационно-программному обеспечению	В течение месяца со дня выявления
7.	Общий бесконтрольный доступ к файлам или папкам, размещенным на АРМ, со сторонних АРМ	Установить модель доступа к ресурсам АРМ, которая требует обязательного прохождения процедуры авторизации. Установить запрет на бесконтрольное разрешение общего доступа к файлам или папкам, размещенным на АРМ, для сторонних АРМ	Специалист по информационно-программному обеспечению	В течение недели со дня выявления
8.	Отключение обновления ОС	Настроить автоматическое обновление ОС в режиме, обеспечивающем эффективное	Специалист по информационно-программному обеспечению	В течение недели со дня выявления

		исполнение служебной деятельности. В случае затруднения работы на АРМ при включенном автоматическом режиме обновления ОС необходимо настроить уведомления о скачанных обновлениях с предложением установки		
9.	Разрешение удаленного управления АРМ средствами ОС	Установить запрет на удаленное управление АРМ средствами ОС	Специалист по информационно-программному обеспечению	В течение 3 рабочих дней со дня выявления
10.	Использование программных средств для предоставления или получения удаленного доступа к АРМ (в том числе AmmyyAdmin, TeamViewer)	Удалить ПОдля предоставления или получения удаленного доступа к АРМ (в том числе TeamViewer)	Специалист по информационно-программному обеспечению	В течение 3 рабочих дней со дня выявления
11.	Установка нелицензионного ПО	Удалить ПО, не имеющее лицензий, и установить на АРМ лицензионное ПО	Специалист по информационно-программному обеспечению	В течение недели после закупки
12.	Установка ПО неслужебного характера	Запретить самостоятельную установку пользователям АРМ программных продуктов	Специалист по информационно-программному обеспечению	В течение недели со дня выявления
13.	Размещение на локальных дисках АРМ информации неслужебного характера	Провести инструктаж пользователей АРМ о запрете размещения любых файлов и папок на системном диске (диске, на котором установлена ОС) и неслужебной информации на всех дисках. В случае наличия только системного диска	Специалист по информационно-программному обеспечению	В течение недели со дня выявления

		создать новый логический диск. Периодически осуществлять контроль за данными, размещенными на логических дисках		
14.	Посещение интернет-ресурсов, не относящихся к служебной деятельности пользователя АРМ (в том числе социальные сети)	Аппаратными или программными средствами (в частности, антивирусным ПО) заблокировать доступ к интернет-ресурсам, не относящимся к служебной деятельности пользователя АРМ	Специалист по информационно-программному обеспечению	В течение недели со дня выявления

Приложение N 4
к требованиям к оснащению
автоматизированных рабочих мест
Администрации Большесолдатского района
Курской области и
порядку их использования

ПАСПОРТ
автоматизированного рабочего места

Аппаратная конфигурация:

Наименование	Марка, модель, конфигурация	Инв. номер
Системный блок модель/ЦП/ОЗУ/HDD/Video		
Монитор		
Принтер		
Сканер		

Программное обеспечение:

Наименование	Версия / лицензия	Ключ/ Код регистрации
Операционная система		
Офисный пакет		
Антивирус		
Интернет (браузер)		
СЗИ		

Настройки пользователя:

Наименование	Информация	прим.
Место установки	Структурное подразделение, N кабинета	
Ответственный пользователь	Ф.И.О, номер телефона	
Сетевое имя АРМ/сетевой		

адрес		
Имя учетной записи пользователя		
Общие ресурсы		

Дата первичной настройки: _____

Ответственное лицо, проводившее настройку: _____/_____/

Работы с АРМ и изменения, вносимые в состав и настройку АРМ:

Дата изменения	Информация о проведенной работе	Результат проведенной работы	ФИО и подпись лица, проводившего работу