Приложение № 14

к Регламенту удостоверяющего  
центра БУЗОО «МИАЦ»   
(VPN № 798)

ИНСТРУКЦИЯ

абонента Удостоверяющего центра бюджетного учреждения здравоохранения Омской области «Медицинский информационно-аналитический центр»

1. Общие положения
   1. Данная Инструкция абонента Удостоверяющего центра бюджетного учреждения здравоохранения Омской области «Медицинский информационно-аналитический центр» (далее – Инструкция) разработана для создания необходимых условий для функционирования защищенной ведомственной сети передачи данных и создания системы защищенного юридически значимого электронного документооборота с применением электронной подписи в учреждениях, подключенных к Удостоверяющему центру бюджетного учреждения здравоохранения Омской области «Медицинский информационно-аналитический центр» (далее – Учреждения).
   2. Инструкция разработана в соответствии с требованиями Федеральных законов от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи», от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и других федеральных законах.
   3. Инструкция предназначена для должностных лиц Учреждения, являющихся владельцами сертификатов ключей проверки электронной подписи (далее – СКПЭП), изданных Удостоверяющим центром бюджетного учреждения здравоохранения Омской области «Медицинский информационно-аналитический центр» (далее – УЦ БУЗОО «МИАЦ»), и зарегистрированных на абонентских пунктах (далее − АП) сети ViPNet VPN № 798 защищенной сети передачи данных (далее – ЗСПД) БУЗОО «МИАЦ» и определяет их ответственность при работе с конфиденциальной (в том числе ключевой) информацией, их права и полномочия, а также порядок исполнения своих обязанностей на различных этапах эксплуатации ЗСПД БУЗОО «МИАЦ».

2. Назначение и функции программного обеспечения абонентского пункта

2.1. Основу информационного обеспечения Учреждения для решения стоящих перед ними задач составляет межсетевой обмен информацией конфиденциального характера, которая в соответствии с федеральным и региональным законодательством и ведомственными нормативно-правовыми актами Учреждения подлежит защите.

2.2. Главный принцип защиты – в любых условиях деятельности Учреждения информация конфиденциального характера с ограниченным доступом должна быть защищена с целью сохранения основных ее свойств: конфиденциальности, достоверности, целостности и доступности. При этом указанная информация подлежит защите при ее передаче по всем типам каналов связи, используемым в ЗСПД БУЗОО «МИАЦ», независимо от их принадлежности и условий предоставления.

2.3. К числу основных угроз безопасности конфиденциальной информации, хранимой и обрабатываемой в Учреждении, относится несанкционированный доступ и программное воздействие («сетевые атаки») на саму конфиденциальную информацию, а также на программные средства, применяемые для ее обработки, со стороны пользователей глобальной информационной сети Интернет. В связи с этим межсетевой информационный обмен данными в рамках ЗСПД БУЗОО «МИАЦ» должен осуществляться в защищенном режиме.

2.4. ПО ViPNet [Клиент] устанавливается на абонентский пункт (далее – АП) Учреждения, когда требуется решение следующих задач:

* на АП сотрудника Учреждения обрабатывается важная информация, требующая защиты от возможного несанкционированного доступа из внутренних локально вычислительной сети (далее − ЛВС) Учреждения всех уровней, в том числе и со стороны системных администраторов;
* удаленное подключение компьютера в составе ЛВС Учреждения, если в ней отсутствует координатор;
* удаленное подключение компьютера (в т.ч. мобильного), находящегося вне ЛВС Учреждения, защищенной координатором.

2.5. При отсутствии координатора на границе ЛВС Учреждения, программного обеспечения (далее – ПО) ViPNet [Клиент] является основным средством для сетевой защиты обмена данными рабочих станций сотрудников Учреждения, работающими с общими ресурсами на серверах в режиме удалённого доступа.

3. Ответственность пользователя

3.1. Пользователь назначается приказом руководителя Учреждения эксплуатации ПО АП и несет ответственность за:

* обеспечение своевременного получения и отправки ЭД Учреждения, в том числе в режиме автоматической обработки файлов и входящих ЭД (обмен данными серверов баз данных);
* конфиденциальность, достоверность, целостность и доступность информации конфиденциального характера, обрабатываемой на его АП и передаваемой на другие объекты защищенной сети под его паролем;
* поддержание архива переданных и полученных средствами АП ЭД в актуальном состоянии;
* своевременность плановой смены пароля для запуска ПО АП и ключевой информации АП в соответствии с установленной в Учреждении периодичностью;
* отсутствие на АП вредоносных программ (компьютерных «вирусов», «троянских коней», «программ-закладок» и т.п.);
* достоверность информации, представляемой доверенному лицу УЦ, АП для включения в СКПЭП при его издании;
* своевременность отправки заявки в УКЦ на новый СКПЭП при изменении содержащейся в нем информации или выявлении ее несоответствия информации, представленной доверенному лицу УЦ при его издании;
* соблюдение требований конфиденциальности ключевой информации на всех этапах функционирования сети ViPNet VPN № 798.

Пользователь несет персональную ответственность за сохранение в тайне от кого бы то ни было собственного, известного только ему, пароля для запуска ПО АП, и недоступность посторонним лицам ключевой информации АП, зашифрованной на его парольном ключе.

3.2. Пользователю запрещается:

* отменять ввод пароля для входа в ПО АП при включении (перезагрузке) компьютера или иным способом отключать программные средства защиты информации во время решения задач конфиденциального характера;
* допускать к решению задач конфиденциального характера на своем рабочем месте лиц, не имеющих к ним отношения и не включенных в списки пользователей, допущенных к конфиденциальной информации в Учреждении;
* передавать пароли (парольные фразы) в открытом виде кому бы то ни было, включая своих руководителей, администратору информационной безопасности, Администратора безопасности УЦ БУЗОО «МИАЦ», доверенное лицо УЦ БУЗОО «МИАЦ», представителям сторонних организаций, осуществляющих техническую поддержку (сопровождение) ПО, установленного на АП;
* покидать свое рабочее место с незаблокированным включенным компьютером;
* осуществлять попытки входа в сеанс связи с другими информационными системами и сетями, не входящими в состав ЗСПД Учреждения;
* самостоятельно изменять настройки фильтров, режимов и другие настройки безопасности ПО АП, а также настройки сетевого подключения своего АП к ЛВС Учреждения, хотя бы они и были ему доступны по его уровню полномочий;
* самостоятельно устанавливать дополнительное программное и информационное обеспечение, разработанное самостоятельно или полученное из сторонних источников без согласования, в том числе компьютерные игры, тренажеры, обучающие и справочно-информационные программы, программы для изменения свойств рабочего стола Windows и т.п.;
* предоставлять посторонним лицам какие-либо сведения об операционной системе и другом общесистемном программном обеспечении, в том числе технических средствах защиты информации, установленных на рабочих станциях и серверах Учреждения, а также об их настройках.

4. Права пользователя

4.1. Пользователь в процессе повседневной эксплуатации ПО АП имеет право:

* сменять пароль для запуска ПО АП до истечения срока его действия по своему усмотрению;
* с целью обеспечения конфиденциальности при смене пароля для запуска ПО АП требовать от других лиц покинуть помещение, в котором установлен АП, на время процедуры смены пароля;
* устанавливать срок действия собственного пароля для запуска ПО АП по своему усмотрению, но не более одного года;
* сменять СКПЭП до истечения срока его действия по своему усмотрению;
* с целью повышения удобства пользования списком доступных ему узлов защищенной сети упорядочивать его с помощью создания именованных по своему усмотрению папок и использования по своему усмотрению сервиса псевдонимов;
* с целью повышения удобства пользования почтовым ящиком Деловой почты упорядочивать его с помощью создания именованных по своему усмотрению папок;
* с целью повышения удобства пользования адресной книгой Деловой почты упорядочивать ее с помощью создания списков рассылки;
* с целью оперативного разрешения внезапно возникающих проблем, в том числе при использовании ПО АП, использовать по своему усмотрению предоставляемые ПО АП сервисы защищенного оперативного обмена сообщениями и защищенной конференции, а также файлового обмена;
* с целью оперативного разрешения внезапно возникающих проблем при использовании ПО АП, обращаться в УЦ БУЗОО «МИАЦ», а также в организацию-поставщик ПО, осуществляющую его техническую поддержку и сопровождение, по любым доступным ему каналам доступа – по телефону или факсу, с использованием предоставляемых ПО АП сервисов защищенного оперативного обмена сообщениями или защищенной конференции, файлового обмена или Деловой почты.

4.2. Должностным лицам Учреждения запрещается:

* требовать от пользователя предоставления известных только ему паролей (парольных фраз);
* производить подбор паролей для входа в ПО АП;
* требовать от пользователя предоставления возможности работать на его АП под его паролем в его отсутствие;
* запускать ПО АП под чужим паролем;
* требовать от пользователя предоставления каких-либо сведений об используемых на его АП средствах защиты информации, кроме изложенных в настоящей Инструкции (в том числе и при проведении периодической аттестации).

4.3. Для формирования или изменения списка связей в ЗСПД БУЗОО «МИАЦ», Учреждению необходимо направить в УЦ БУЗОО «МИАЦ» заявление на добавление связей для узла ЗСПД БУЗОО «МИАЦ» (Приложение № 1 к настоящей Инструкции).

При необходимости организации связи с узлом ЗСПД внешнего УЦ требуется дополнительное согласование данной связи в соответствии с регламентом внешнего УЦ.

5. Обязанности должностных лиц учреждения при их регистрации в качестве пользователя ЗСПД БУЗОО «МИАЦ»

Должностное лицо Учреждения, утвержденное в качестве пользователей ЗСПД БУЗОО «МИАЦ» обязано:

5.1. В согласованные с УЦ БУЗОО «МИАЦ» прибыть лично или направить своего представителя для прохождения инструктажа по правилам обращения с ключевой информацией и об ответственности за разглашение конфиденциальной информации под роспись в заявление на изготовление СКПЭП (ключевой информации), получения собственного ключевого дистрибутива вместе с паролем доступа к нему под роспись в Журнале учета выдачи ключевой информации. Для аутентификации личности пользователя, при получении ключевого дистрибутива прибывающие в УЦ БУЗОО «МИАЦ» должностные лица должны иметь при себе личный паспорт гражданина Российской Федерации или иной документ, законодательно признаваемый в качестве документа, удостоверяющего личность, а в случае, если вместо пользователя в УЦ БУЗОО «МИАЦ» прибывает его представитель – доверенность пользователя на получение ключевой информации.

При первоначальном развертывании АП ЗСПД БУЗОО «МИАЦ», а также после компрометации закрытых (секретных) ключей подписи пользователей, зарегистрированных на АП, производится установка ПО ViPNet [Клиент] на АП с использованием выдаваемых пользователям ключевых дистрибутивов администратором безопасности Учреждения или иной организацией на договорной основе имеющий соответствующую лицензию ФСБ.

При регистрации нового пользователя на уже существующем АП ключевой дистрибутив пользователю выдаётся на машинном носителе ключевой информации в зашифрованном на парольном ключе для первого входа пользователя в систему виде.

5.2. При регистрации нового пользователя на уже существующем АП самостоятельно или с помощью администратора безопасности Учреждения запустить ПО АП с использованием выданного ему в УЦ пароля для первого входа в систему, по запросу АП вставить машинный носитель ключевой информации (дискету, flash и т.д.) с собственным ключевым дистрибутивом в зашифрованном на парольном ключе виде, и после расклейки (переноса) ключевой информации на жесткий диск АП вынуть машинный носитель ключевой информации и уничтожить ключевой дистрибутив способом физического разрушения машинного носитель ключевой информации или иным предусмотренным документацией способом с оформлением акта (Приложение № 5 к настоящей Инструкции). Один экземпляр акта уничтожения ключевого дистрибутива направить в БУЗОО «МИАЦ».

5.3. В ходе первого сеанса работы на своем АП согласно эксплуатационно-технической документации организации-разработчика ПО ViPNet сформировать новый, известный только ему личный пароль, записать его (парольную фразу) на бумажный носитель и ввести его в действие. Действующий пароль на бумажном носителе поместить в непрозрачный конверт, конверт заклеить и опечатать по месту склейки не менее чем двумя оттисками печати Учреждения. На конверте сделать запись, идентифицирующую его содержимое, а также дату и время ввода пароля в действие, например: «КОНФИДЕНЦИАЛЬНО! Пароль для АП ViPNet c 13.00 14.06.2009». Данную запись удостоверить собственноручной подписью.

5.4. В ходе первого сеанса работы на своем АП согласно эксплуатационно-технической документации организации-разработчика ПО ViPNet отправить электронный запрос на СКПЭП с новым ключом проверки электронной подписи в УКЦ для получения СКПЭП (запрос формируется ПО АП, при этом автоматически вырабатываются новые ключи подписи пользователя). Запрос автоматически подписывается ЭП пользователя с использованием ключей подписи, выданных ему в составе ключевого дистрибутива.

5.5. После получения электронной квитанции о доставке электронного запроса в УКЦ, оформить и распечатать два экземпляра Заявления на СКПЭП, где уточнить свои реквизиты, указанные в электронном запросе. Подписать их собственноручной подписью.

5.6. Прибыть лично с документами, оформленными и распечатанными согласно Регламенту УЦ БУЗОО «МИАЦ» (VPN № 798) (далее – Регламент) к доверенному лицу УЦ для получения СКПЭП на бумажном носителе. Для аутентификации личности владельца СКПЭП при получении СКПЭП на бумажном носителе прибывающие в УЦ должностные лица должны иметь при себе личный паспорт гражданина Российской Федерации или иной документ, законодательно признаваемый в качестве документа, удостоверяющего личность. При необходимости (если владельцем СКПЭП выступает должностное лицо, неуполномоченное положением об Учреждении вести переписку от имени Учреждения), оформляется доверенность Учреждения на подписание электронных документов (Приложение № 2 к настоящей Инструкции).

Доверенное лицо УЦ регистрирует электронный запрос на СКПЭП в качестве СКПЭП и распечатывает два экземпляра СКПЭП на бумажном носителе установленной формы (согласно Регламенту). Владелец СКПЭП или его представитель сверяет их с имеющимися у него распечатками заявки на СКПЭП. Доверенное лицо УЦ проставляет в Заявлении уникальный регистрационный номер, присвоенный СКПЭП при его издании. Заявление и СКПЭП на бумажных носителях по форме согласно Регламенту. СКПЭП на бумажном носителе заверяется собственноручной подписью владельца СКПЭП или его представителя. Один экземпляр оформленных документов передается владельцу СКПЭП или его представителю. Второй экземпляр хранится в БУЗОО «МИАЦ».

5.7. После получения электронной квитанции об удовлетворении в УКЦ электронного запроса на СКПЭП, ввести полученный на АП СКПЭП в действие.

6. Обязанности пользователя по юридически значимому информационному обмену электронными документами

Пользователь ЗСПД в процессе повседневной деятельности обязан:

6.1. Знать комплектацию и исходное состояние технических средств АП, в том числе количество и назначение всех соединительных проводов (кабелей); ежедневно по прибытию на свое рабочее место осматривать АП на предмет доступа к нему посторонних лиц, при этом проверять правильность опечатывания системного блока, правильность и надежность крепления в соответствующих разъемах штатных (предусмотренных эксплуатационной документацией на АП) проводов (кабелей). Особое внимание обращать на сетевой кабель для подключения рабочей станции к ЛВС Учреждения, и модем с комплектом кабелей для подключения к сети Интернет. В случае обнаружения признаков несанкционированного доступа посторонних лиц к АП, наличия посторонних (не упоминаемых в эксплуатационной документации АП) или свободных (не присоединенных к соответствующим разъемам) проводов (кабелей) и устройств, немедленно поставить об этом в известность своего руководителя и администратора информационной безопасности своего Учреждения и действовать согласно их указаниям.

6.2. Знать порядок и правила запуска ПО АП, операционной системы (далее − ОС), подключения к ЛВС и Интернет, антивирусного ПО, необходимых прикладных программ. Включать рабочую станцию согласно эксплуатационной документации и вводить собственный, известный только ему пароль для запуска ПО АП. В случае отклонений от привычного порядка загрузки ПО АП, ОС и другого установленного на АП ПО, немедленно поставить об этом в известность своего руководителя и администратора информационной безопасности своего Учреждения и действовать согласно их указаниям.

6.3. Уходя со своего рабочего места по окончанию рабочего дня (или, при необходимости, на достаточно длительное время), выключать рабочую станцию согласно эксплуатационной документации.

6.4. Уходя со своего рабочего места на небольшой срок, блокировать компьютер.

6.5. Организовывать установленным в Учреждении порядком юридически значимой электронной переписки сбор информации от сотрудников для передачи в другим пользователям Учреждения и сторонним организациям, ее представление на утверждение (подпись, визирование) руководителю АП Учреждения, оформление в виде исходящих ЭД, помещение исходящих ЭД в очередь транспортного модуля ПО АП и рекомендуется их регистрация в Журнале исходящих электронных документов (Приложение № 3 к настоящей Инструкции).

6.6. При получении из УЦ БУЗОО «МИАЦ» обновлений ключевой и адресной информации проводить её обновление средствами ПО АП по возможности немедленно, но во всяком случае не позднее дня получения такого обновления.

6.7. Контролировать получение электронных квитанций (извещений) о доставке и прочтении адресатами отправленных исходящих ЭД, рекомендуется регистрировать их получение в Журнале исходящих электронных документов (Приложение № 3 к настоящей Инструкции). В случае неоправданной задержки прочтения и исполнения адресатами принимать соответствующие меры.

6.8. Проверять ЭП полученных ЭД средствами АП, в случае получения ЭД, подпись которых недействительна, немедленно оповещать об этом администратора безопасности УЦ БУЗОО «МИАЦ» и далее действовать согласно его указаниям.

6.9. Полученные ЭД, подпись которых действительна, рекомендуется регистрировать в Журнале входящих электронных документов (Приложение № 4 к настоящей Инструкции), при необходимости распечатывать вложения, и установленным в органе Учреждения порядком юридически значимой электронной переписки представлять полученные ЭД в электронном виде или в твердой копии на бумажном носителе руководителю Учреждения для изучения и принятия решения (наложения резолюции, оформления поручения должностным лицам Учреждения) по порядку их исполнения и контроля исполнения.

6.10. В соответствии с установленным в органе Учреждения порядком ведения архива юридически значимой электронной переписки осуществлять копирование (сохранение) полученных ЭД с отсоединенной подписью на машинные носители информации (в папки на локальных жестких дисках АП и сетевых дисках ЛВС, на съемные носители – дискеты, магнитооптические, CD- и DVD-диски, для кратковременного хранения – на устройства флэш-памяти) для обеспечения возможности изучения и работы с полученными ЭД должностных лиц Учреждения.

6.11. Осуществлять резервное копирование (сохранение) отправленных ЭД с присоединенной подписью на машинные носители информации (в папки на локальных жестких дисках АП и сетевых дисках ЛВС, на съёмные носители – дискеты, магнитооптические, CD- и DVD-диски, для кратковременного хранения – на устройства флэш-памяти) для обеспечения невозможности их случайного или преднамеренного изменения.

7. Обязанности пользователя по смене паролей для запуска ПО АП

7.1. Пользователи обязаны производить периодическую (плановую) смену своих собственных, известных только им паролей для запуска ПО АП не реже срока действия пароля, задаваемого средствами ПО АП и установленного в УЦ БУЗОО «МИАЦ» в один год. Программное обеспечение АП заблаговременно информирует пользователя о необходимости проведения данной процедуры.

7.2. Смена пароля для запуска ПО АП также может осуществляться пользователем по собственной инициативе в любое время.

7.3. Пользователи обязаны производить смену пароля для запуска ПО АП до истечения срока его действия в следующих случаях:

* после проведения настройки общесистемного или прикладного программного обеспечения иными сотрудниками (например, после ремонта рабочей станции и ее комплектующих);
* при назначении руководителем Учреждения другого должностного лица временно исполнять обязанности пользователя в случае его длительного отсутствия (отпуска, командировки, обучения, заболевания и т.п.) и возобновлении исполнения пользователем своих обязанностей после его возвращения;
* после вскрытия конверта с паролем, сданного пользователем руководителю Учреждения на ответственное хранение, как самим пользователем, так и комиссионно другими уполномоченными на это должностными лицами;
* по указанию администратора безопасности УЦ БУЗОО «МИАЦ» (например, в случае компрометации парольной документации).

7.4. В ходе процедуры смены пароля для запуска ПО АП пользователь обеспечивает конфиденциальность данной процедуры, при необходимости удалив из помещения, в котором установлен АП, других лиц, согласно эксплуатационно-технической документации организации-разработчика ПО ViPNet формирует новый, известный только ему личный пароль, записывает его (или соответствующую ему парольную фразу) на бумажный носитель и вводит его в действие. Действующий пароль на бумажном носителе помещается в непрозрачный конверт, конверт заклеивается и опечатывается по месту склейки не менее чем двумя оттисками печати Учреждения. На конверте делается запись, идентифицирующая его содержимое, а также дату и время ввода пароля в действие, например*:* «КОНФИДЕНЦИАЛЬНО! Пароль для АП ViPNet c 13.00 14.06.2009». Данную запись удостоверяется собственноручной подписью пользователя.

Запечатанный конверт с действующим паролем на бумажном носителе хранится в безопасном месте, например, в опечатываемом сейфе. Если опечатываемый сейф у пользователя не предусмотрен, допускается его хранение в сейфе руководителя подразделения пользователя (руководителя Учреждения) или администратора безопасности Учреждения.

При помещении в сейф нового конверта с действующим паролем на бумажном носителе конверт с паролем, утратившим действие, из сейфа изымается и уничтожается.

8. Обязанности владельца СКПЭП при прекращении исполнения им служебных обязанностей

8.1. Владелец СКПЭП в случае прекращения исполнения им служебных обязанностей (при его увольнении, переводе на другую должность, в том числе в другое подразделение Учреждения) обязан направить доверенному лицу УЦ БУЗОО «МИАЦ» заявку на аннулирование (отзыв) СКПЭП (согласно Регламенту).

8.2. Заявка на отзыв СКПЭП направляется: в электронном виде с АП владельца СКПЭП (заверяется его ЭП), и на бумажном носителе (заверяется рукописной подписью владельца СКПЭП) с сопроводительным письмом за подписью руководителя Учреждения.

\_\_\_\_\_\_\_\_\_\_\_\_

Приложение № 1

к Инструкции абонента Удостоверяющего центра БУЗОО «МИАЦ»

|  |  |
| --- | --- |
| На бланке организации | Директору БУЗОО «МИАЦ» |

Заявление

на добавление связей для узла \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ сети VPN № 798

(наименование узла ЗСПД БУЗОО «МИАЦ»)

, (далее − Учреждение),

(наименование юридического лица)

в лице ,

(наименование должности, фамилия, имя, отчество лица, уполномоченного выдавать доверенности)

действующего на основании \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, в связи

(наименование документа, подтверждающего полномочия заявителя)

с\_\_\_\_\_\_\_\_\_\_\_\_\_\_ просит добавить в список связей ЗСПД БУЗОО «МИАЦ» следующие узлы:

(указать причину)

|  |  |  |
| --- | --- | --- |
| № п/п | Наименование узла защищенной сети передачи данных БУЗОО «МИАЦ» (или учреждения) | Основание (дата номер соглашения об информационном обмене) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Должность руководителя \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /

М.П.

"\_\_" \_\_\_\_\_\_\_ 20\_\_\_ г.

Отметка о согласовании:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | Приложение № 2  к Инструкции абонента  Удостоверяющего центра БУЗОО «МИАЦ» |
| Угловой штамп юридического лица, дата и регистрационный номер |  |

ДОВЕРЕННОСТЬ

на подписание электронных документов

, (далее − Учреждение),

(наименование юридического лица)

в лице ,

(наименование должности, фамилия, имя, отчество лица, уполномоченного выдавать доверенности)

действующего на основании ,

(наименование документа, согласно которому предоставлены такие полномочия)

уполномочивает

(должность, фамилия, имя, отчество уполномоченного представителя юридического лица)

паспортные данные:

(наименование документа, серия, номер, дата выдачи, орган, выдавший документ)

телефон для связи:

от имени и в интересах организации подписывать исходящие электронные

документы при выполнении действий в соответствии с

(наименование законодательного

,

или иного нормативного акта, в соответствии с которым осуществляется электронный документооборот)

Настоящая доверенность действительна до “ ” 20\_\_ года.

(должность уполномоченного вести переписку юридического лица)

“\_\_\_\_” \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20 \_\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ / \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/

М.П.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | Приложение № 3  к Инструкции абонента Удостоверяющего центра БУЗОО «МИАЦ» |

Журнал

исходящих электронных документов

*(левая, чётная страница)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Регистрационный номер | Тема | Исполнитель | Краткое содержание документа | Атрибуты | |
| Вложения | П | Ш |
| 1 | 2 | 3 | 4 | 5 | 6 |
|  |  |  |  |  |  |

*(правая, нечётная страница)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Дата и время отправления | Размер | Список получателей | Дата и время извещений | | Примечание (принятые меры) |
| о доставке | о прочтении |
| 7 | 8 | 9 | 10 | 11 | 12 |
|  |  |  |  |  |  |

Примечания по ведению журнала:

Для каждого абонентского пункта (далее – АП) Учреждения заводится отдельный Журнал исходящих электронных документов. Если на АП зарегистрировано несколько пользователей, то при большом объёме передаваемой информации допускается заводить по отдельному журналу на каждый коллектив пользователей.

В графе 1 проставляется регистрационный номер отправленного документа в соответствии с графой «Регистрационный номер» папки «Исходящие» главного окна «Деловой почты».

В графе 2 в первой из строк, отведённых отправленному документу, указывается тема письма (документа). В следующих строках перечисляются имена файлов вложений.

В графе 3 в первой из строк, отведённых отправленному документу, указывается фамилия и инициалы исполнителя, готовившего текст письма (документа). В следующих строках перечисляются фамилии и инициалы исполнителей, готовивших каждый из соответствующих файлов вложений, указанных в графе 2.

В графе 4 указывается краткое содержание отправленного документа, а если документ содержит вложения — и краткое описание файлов вложений.

В графах 5 и 6 в первой из строк, отведённых отправленному документу, проставляются атрибуты отправленного документа (письма): «П» – отметка о подписании письма; «Ш» – отметка об отправке документа (письма) в зашифрованном виде. В следующих строках проставляются атрибуты «П» и «Ш» соответствующих файлов вложений.

В графе 7 указывается дата и время отправки документа (письма) в соответствии с графой «Дата создания» папки «Исходящие» главного окна «Деловой почты».

В графе 8 в первой из строк, отведённых отправленному документу, проставляется общий объём отправленного документа (письма), в следующих – размеры соответствующих вложений.

В графе 9 перечисляются все адресаты документа (письма) в соответствии со списком рассылки документа (письма). Каждому адресату (получателю) соответствует отдельная строка.

В графе 10 проставляются дата и время получения извещения о доставке (AD) документа (письма) соответствующему адресату из графы 9 согласно папке «Входящие\Извещения»

В графе 11 проставляются дата и время получения извещения о прочтении (AR) документа (письма) соответствующим адресатом из графы 9 согласно папке «Входящие\Извещения».

В графе 12 при необходимости указываются меры, предпринятые пользователем в случае задержки получения квитанций о доставке и прочтении документов (писем).

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | Приложение № 4  к Инструкции абонента Удостоверяющего центра БУЗОО «МИАЦ» |

Журнал

входящих электронных документов

*(левая, чётная страница)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Регистрационный номер | Атрибуты | | Дата и время получения | От кого получено | Тема | Размер |
| П | Ш | Вложения |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|  |  |  |  |  |  |  |

*(правая, нечётная страница)*

|  |  |  |  |
| --- | --- | --- | --- |
| Краткое содержание документа | Кому передано на исполнение | Папка архивного хранения | Примечание |
| 8 | 9 | 10 | 11 |
|  |  |  |  |

Примечания по ведению журнала:

Для каждого абонентского пункта (далее – АП) Учреждения заводится отдельный Журнал входящих электронных документов. Если на АП зарегистрировано несколько пользователей, то при большом объёме принимаемой информации допускается заводить по отдельному журналу на каждый коллектив пользователей.

В графе 1 проставляется регистрационный номер полученного документа (письма) в соответствии с графой «Регистрационный номер» папки «Входящие» главного окна «Деловой почты».

В графах 2 и 3 в первой из строк, отведённых полученному документу, проставляются атрибуты полученного документа (письма): «П» – результат проверки подписи; «Ш» – отметка о получении документа (письма) в зашифрованном виде. В следующих строках проставляются атрибуты «П» и «Ш» соответствующих файлов вложений согласно их расположению в графе 6.

В графе 4 указывается дата и время получения документа (письма) в соответствии с графой «Дата получения» папки «Входящие» главного окна «Деловой почты».

В графе 5 в первой из строк, отведённых полученному документу, указывается, кем подписано письмо (документ). Если вложения подписаны иным пользователем, то в соответствующих строках указывается, кем подписаны эти вложения.

В графе 6 в первой из строк, отведённых полученному документу, указывается тема письма (документа). В следующих строках перечисляются имена файлов вложений.

В графе 7 в первой из строк, отведённых полученному документу, проставляется общий объём полученного документа (письма), в следующих – размеры соответствующих вложений.

В графе 8 указывается краткое содержание полученного документа, а если документ содержит вложения – и краткое описание файлов вложений.

В графе 9 в первой из строк, отведённых полученному документу, указывается фамилия и инициалы руководителя Учреждения, которому представлен полученный документ (письмо) для изучения и принятия решения о его исполнении. В следующих строках перечисляются фамилии и инициалы сотрудников Учреждения, которым в соответствии с резолюцией (поручением) руководителя переданы для исполнения соответствующие файлы вложений.

В графе 10 в первой из строк, отведённых полученному документу, указывается, в какой папке (на локальном или сетевом диске, на CD- или DVD-диске) и под каким именем сохранено полученное письмо (документ), в следующих строках перечисляются папки (на локальном или сетевом диске, на CD- или DVD-диске), куда сохранены резервные юридически значимые копии файлов вложений.

В графе 11 при необходимости проставляется дата и время удаления полученного письма из почтовой базы деловой почты.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
|  | Приложение № 5  к Инструкции абонента  Удостоверяющего центра БУЗОО «МИАЦ» |

Утверждаю

Руководитель

(наименование Учреждения)

(подпись, расшифровка подписи)

« « 20 г.

АКТ

уничтожения машинных носителей ключевой информации

Комиссия в составе

(фамилии, инициалы, наименование должностей членов комиссии)

произвела отбор машинных носителей ключевой информации, использованных по назначению, для их уничтожения. Комиссия установила:

1. Уничтожению подлежат машинных носителей ключевой информации,  
использованных по назначению, за учётными номерами:   
 .

2. машинных носителей ключевой информации, использованных по  
назначению, за учётными номерами:   
 физически уничтожены  
путём вскрытия и разрушения футляра дискеты, извлечения дискеты и разрезания её ножницами на сегменты. Обломки футляра и сегменты дискеты утилизированы.

Настоящий акт составлен в двух экземплярах:

1 экземпляр — направляется в УЦ БУЗОО «МИАЦ»;

2 экземпляр — \_\_\_\_\_\_.

Члены комиссии:

(роспись, инициалы, фамилия)

“ ” 20 г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_