# СТО 070-017-2019. Система менеджмента. ТЕХНИЧЕСКОЕ УПРАВЛЕНИЕ ЭЛЕКТРОННЫМИ СРЕДСТВАМИ

1. СТО 070-017-2019. Система менеджмента. Техническое управление электронными средствами

1 РАЗРАБОТАН главным специалистом ЗАО «М-Стандарт»

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом генерального директора ЗАО «М-Стандарт» от 06.05.2019 № 117-од. Дата введения 20.05.2019

3 РАЗРАБОТАН в развитие требований Критериев аккредитации, утв. Приказом Минэкономразвития № 326 от 30.05.2014, ГОСТ ИСО/МЭК 17025-2009 п.п. 5.4.7, ГОСТ Р ИСО 9001-2015 п. 7.1.3, п. 7.1.6, п. 7.3, п. 7.4 с учетом положени, ГОСТ Р 54471-2011/ ISO/TR 15801:2009, ГОСТ Р ИСО/МЭК 27001-2006 применительно к деятельности ЗАО «М-Стандарт».

4 ВВЕДЕН ВЗАМЕН СТО 070-017-2015.

5 Переиздание в редакции изменения № 1, принятого в декабре 2019 г.

1 Область применения

Настоящий стандарт определяет процедуру управления электронными средствами, используемыми в деятельности ЗАО «М-Стандарт».

Действие настоящего стандарта распространяется на весь ЗАО «М-Стандарт», использующий в работе электронные средства.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие документы:

Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 (в ред. от 21.07.2014 № 242-ФЗ)

Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 (в ред. от 18.03.2019 N 31-ФЗ)

Федеральный закон «Об электронной подписи» № 63-ФЗ от 06.04.2011 (в ред. от 23.06.2016 [N 220-ФЗ](consultantplus://offline/ref=1751A265FEF22AE303E899DE6A938A158DA9D714FBED82D32663A6C7A6D6D2C0E7DD18403FFB99B5h745M)[)](consultantplus://offline/ref=4B925BEB05AE4E53B7E02291DF59CF22D764F5875E93D6E47E755158E1746EA79A41C6743F383D29u8LAD)

ГОСТ 19.201-78 Единая система программной документации. Техническое задание. Требования к содержанию и оформлению

ГОСТ 34.602-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ Р ИСО 9000-2015 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 9001-2015 Системы менеджмента качества. Требования

ГОСТ ИСО/МЭК 17025-2009 Общие требования к компетентности испытательных и калибровочных лабораторий

ГОСТ Р 54471-2011/ ISO/TR 15801:2009 Управление документацией. Информация, сохраняемая в электронном виде. Рекомендации по обеспечению достоверности и надежности

ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования

ГОСТ Р ИСО/МЭК 27000-2012 Системы менеджмента информационной безопасности. Общий обзор и терминология

ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ПП 070-001-2014 Положение об обеспечении соблюдения принципов беспристрастности конфиденциальности и открытости при проведении работ по оценке соответствия в ЗАО «М-Стандарт»

СТО 070-001-2016 Система менеджмента ЗАО «М-Стандарт» в области обеспечения качества работ (услуг). Структура и основные положения

СТО 070-003-2017 Управление несоответствиями и неблагоприятными ситуациями

СТО 070-004-2015 Внутренние аудиты (проверки)

СТО 070-005-2014 Управление персоналом

СТО 070-006-2017 Управление документированной информацией

СТО 070-010-2016 Приобретение услуг и материальных ресурсов

Положение о защите персональных данных, утв. Генеральным директором ЗАО «М-Стандарт» 26.08.2015

При пользовании настоящим документом целесообразно проверить действие ссылочных документов в информационных системах: общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодно издаваемому информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году, информационных системах органов государственного управления РФ; внутренних информационных базах данных ЗАО «М-Стандарт». Если ссылочный документ заменен (изменен), то при пользовании настоящим документом следует руководствоваться заменяющим (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения, сокращения

3.1 В настоящем стандарте применены термины с соответст­вующими определениями:

3.1.1 актив: что-либо, что имеет ценность для организации (ГОСТ Р ИСО/МЭК 27000-2012 п. 2.3);

Примечание − Имеются различные типы активов:

- информация;

- программное обеспечение;

- материальные активы, например компьютер;

- услуги;

- люди и их квалификация, навыки и опыт;

- нематериальные активы, такие как репутация и имидж;

3.1.2 доступ к информации: возможность получения информации и ее использования [Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 ст. 2];

3.1.3 информация: Значимые данные (ГОСТ Р ИСО 9000 п. 3.7.1);

3.1.4 информационная безопасность: сохранение конфиденциальности, целостности и доступности информации (ГОСТ Р ИСО/МЭК 27000-2012 п. 2.19);

Примечание - Также сюда могут быть включены другие свойства, такие как подлинность, подотчетность, неотказуемость и достоверность;

3.1.5 информационная система персональных данных: совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств (Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 ст. 3);

3.1.6 контроль доступа: обеспечение того, чтобы доступ к активам был санкционирован и ограничен в соответствии с требованиями коммерческой тайны и безопасности (ГОСТ Р ИСО/МЭК 27000-2012 п. 2.1);

3.1.7 персональные данные: любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных) [Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 ст. 3];

3.1.8 распространение информации: действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

3.1.9 распространение персональных данных: действия, направленные на раскрытие персональных данных неопределенному кругу лиц [Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 ст. 3];

3.1.10 система менеджмента информационной безопасности: часть общей системы менеджмента, основанная на подходе бизнес-рисков по созданию, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению информационной безопасности (ГОСТ Р ИСО/МЭК 27000-2012 п. 2.23);

3.1.11 средства криптографической защиты информации: аппаратные, программные и аппаратно–программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

3.1.12 усиленная квалифицированная электронная подпись: электронная подпись, отвечающая комплексу требований Федерального закона «Об электронной подписи» № 63-ФЗ от 06.04.2011:

получена в результате криптографического преобразования информации с использованием ключа электронной подписи;

позволяет определить лицо, подписавшее электронный документ;

позволяет обнаружить факт внесения изменений в электронный документ после момента его подписания;

создается с использованием средств электронной подписи;

ключ проверки электронной подписи указан в квалифицированном сертификате;

для создания и проверки электронной подписи используются средства электронной подписи, имеющие подтверждение соответствия требованиям, установленным в Федеральнос законе «Об электронной подписи» № 63-ФЗ от 06.04.2011;

3.1.13 электронные средства (электронная оболочка, электронные ресурсы): Технические средства для передачи, хранения, воспроизведения информации, использующие электрические сигналы, математические коды, виртуальное пространство, провода, оптико-волоконные линии, или без направляющих линий;

Примечание - К электронным средствам могут относиться, например, телефон, факсимильный аппарат, сканеры, сервисы электронной почты, ресурсы сети Интернет, сайт организации, флеш-накопители, серверные платформы, принтеры и множительная техника и пр.;

3.1.14 электронная подпись: Информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию (Федеральный закон «Об электронной подписи» № 63-ФЗ от 06.04.2011).

3.2 В настоящем стандарте использованы следующие сокращения:

АСУ - автоматизированные системы управления;

ОУП – отдел управления персоналом;

отдел стандартизации – отдел стандартизации, метрологического обеспечения и экспертных работ

ПК – персональный компьютер;

ПО - программное обеспечение;

ПС – программное средство;

СМ М-Стандарт – система менеджмента ЗАО «М-Стандарт» в области обеспечения качества работ (услуг)

СМИБ – система менеджмента информационной безопасности;

ИБ – информационная безопасность;

СКЗИ – средства криптографической защиты информации;

Средства ЭИ - средства личной электронной идентификации – логин и пароль (дополнительные средства личной электронной идентификации при необходимости), используемые в ЗАО «М-Стандарт»

СТО - стандарт организации;

ЭЦП – усиленная квалифицированная электронная подпись.

4 Организация управления электронными ресурсами

4.1 Обобщенно задачи и основные средства, используемые в построении деятельности по управлению электронными ресурсами приведены в таблице 1.

Таблица 1 - Общее построение деятельности по управлению электронными ресурсами

|  |  |
| --- | --- |
| Решаемые задачи | Обеспечение сохранности документов и данных в электронном виде;  обеспечение передачи информации на расстояние в неизменном (неискаженном виде) виде  Обеспечение внутреннего обмена информацией с достоверной и подтвержденной идентификацией лица (лиц), создающих, распространяющих, изменяющих, хранящих ее составляющие  Обеспечение обмена информацией с заказчиками посредством электронных ресурсов  Обеспечение качественного воспроизведения и размножения информации  Обеспечение достоверной обработки данных и сохранности результатов и данных для решения конкретных задач (расчеты, систематизация данных и пр.)  Обеспечение надлежащего уровня информационной безопасности для электронной информационной среды ЗАО «М-Стандарт». |
| Средства решения задач | Наличие надежно функционирующей внешней и внутренней телефонной сети (IP телефония)  Наличие надежно функционирующих каналов доступа в сеть интернет  Наличие надежно функционирующих каналов внутренней электронной сети (внутренней электронной оболочки, интранет)  Наличие программных средств с опциями создания, накопления, хранения, обмена информацией, в т.ч. документируемой  Функционирование системы менеджмента информационной безопасности  Наличие системы учета, технического обслуживания и проверки работоспособности технических и программных средств электронных ресурсов. |

4.2 Сбор, хранение, систематизация, передача и распространение в электронном виде информации, содержащей персональные данные, осуществляется с соблюдением требований Федерального закона «О персональных данных» № 152-ФЗ от 27.07.2006, внутренних нормативных и организационно-распорядительных документов ЗАО «М-Стандарт», посвященных управлению персональными данными.

4.3 Запросы на выполнение действий по размещению и передаче информации, решение иных задач по передаче, хранению, воспроизведению и обработки информации силами отдела АСУ, направляются начальнику отдела АСУ посредством задач ПС ЭДО 1С согласно СТО 070-006. Записи о направлении, получении, согласовании, исполнении хранятся в электронной базе данных документооборота 1С в течение трех лет.

4.4 Лицом, ответственным за надлежащую организацию технического управления электронными средствами передачи, хранения и воспроизведения информации является начальник отдела АСУ.

5 Телефонная сеть

Основные нормативные положения по использованию телефонной связи приведены в таблице 2.

Таблица 2 - Основные нормативные положения по использованию телефонной связи

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
| Доступность телефонных соединений | Организация телефонной связи осуществляется с использованием IP-сетей (IP — Internet Protocol).  Для телефонной связи используются внешние (принимаются внешние звонки без переадресации) и внутренние телефонные номера (принимаются внутренние звонки и переадресованные внешние звонки).  Каждое производственное помещение оборудуется точкой телефонной связи.  Прием внешних звонков осуществляется преимущественно по единому телефонному номеру, с переадресацией на соответствующие внутренние номера.  Для представителей руководства, руководителей подразделений для пользования в рамках подразделения могут формироваться дополнительные внешние телефонные номера.  Перечень внешних телефонных номеров формируется начальником отдела АСУ по служебным запискам руководителей, утверждается генеральным директором.  Внешняя телефонная связь организуется с использованием услуг провайдеров IP-телефонии. Закупки услуг провайдеров осуществляются в соответствии с СТО 070-010. | Начальник отдела АСУ |
| Оптимизация внешних звонков. | Для оптимизации обработки первичных внешних звонков организуется работа call-центра, который может быть организован на базе технических возможностей и человеческих ресурсов ЗАО «М-Стандарт», с использованием технических возможностей и человеческих ресурсов сторонней организации.  Порядок организации взаимодействия с организацией, предоставляющей услуги call-центра, сотрудниками call-центра – в соответствии с СТО 070-070-016, порядок закупки услуг call-центра – в соответствии с СТО 070-010. | Начальник отдела по работе с клиентами (во взаимодействии с начальником отдела АСУ). |

6 Электронная почта

Основные нормативные положения по использованию электронной почты приведены в таблице 3.

Таблица 3 - Основные нормативные положения по использованию электронной почты

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
|  | 6.1 Политика данных электронной почты.  Политика определяет разрешимое использование электронной почты в сетях предприятия. Такая политика является частью политикой информационной безопасности. |  |
|  | Электронная почта — один из главных методов коммуникации в деловом мире. Это удобно и быстро. Однако есть риски при использовании электронной почты, ибо использование ее небезопасно за пределами информационной сети предприятия. Сообщения отправленные через электронную почту в сеть интернет, могут быть перехвачены, прочитаны или перенаправлены.  Электронная почта ЗАО «М-Стандарт» используется в целях обмена информацией, необходимой для осуществления деятельности ЗАО «М-Стандарт» в рамках функций и обязанностей сотрудника.  Основные положения Политики данных электронной почты:  - все сообщения электронной почты ЗАО «М-Стандарт» (@.uraltest.ru) являются информацией Учреждения;  - электронная почта не используется для пересылки конфиденциальной информации если она не зашифрована специальным ПО, разрешенным для использования в ЗАО «М-Стандарт»;  - запрещается отправка сообщений от чужого имени с почтового ящика, отнесенного к другому лицу;  - при получении сомнительных писем следует обратиться в отдел АСУ не открывая данные сообщения;  - все письма электронной почты предприятия проходят сканирование и могут быть прочтены сотрудниками отдела АСУ ля выявления угроз. Также письма могут помещаться в карантин в автоматическом режиме.  - при составлении писем придерживаются общепринятых правил этикета.  При пользовании сервисами электронной почты запрещается:  - отправка непристойных, оскорбительных, угрожающих или противозаконных материалов;  - рассылка материалов по спискам рассылки (SPAM);  - при получении материалов по спискам рассылки (SPAM) открывать вложения, прикрепленные к письмам; SPAM немедленно удаляется пользователями самостоятельно;  - изменение настроек почтовой программы исполнителем (кроме изменений функциональный опций, предусмотренных почтовой программой для настройки конретными пользователями (подписи, настройки формы представления информации пр.);  - использование электронной почты в личных целях для рассылки и приема электронных сообщений, не касающихся деятельности ЗАО «М-Стандарт» или должностных (функциональных) обязанностей сотрудника, использующего электронную почту.  Отдел АСУ отвечает за соблюдения правил пользования электронной почты каждым сотрудником. Если есть тенденция несоблюдения правил, в его компетенции входит разъяснительные действия с каждым сотрудником предприятия относительно того, какие последствия грозят при недооценки политики безопасности пользованием электронной почтой.  Отдел АСУ отвечает за настройку параметров реализации и обслуживания программного и аппаратного оборудования для работы с электронной почтой. Включая антиспам, антивирус и другие фильтры.  Все сотрудники, которые были осведомлены о данной политике, несут ответственность за соблюдение правил данной политики. Каждый сотрудник в любое время может обратиться в службу информационной безопасности по поводу консультации тех или иных действий относительно политики безопасности пользования электронной почты. |  |
| Доступность связи посредством электронной почты | 6.2 Каждое структурное подразделение, при необходимости – структурное звено имеет адрес электронной почты ЗАО «М-Стандарт» (@uraltest.ru) для использования руководителями и сотрудниками.  Сотрудники ЗАО «М-Стандарт», функциональные обязанности которых включают обмен информацией с представителями заказчиков, внешними организациями могут получать адрес электронной поxты ЗАО «М-Стандарт» (@uraltest.ru).  В случаях замещения руководителей, иных сотрудников в установленном порядке – осуществляется перенаправление сообщений с адреса электронной почты, приписанной сотруднику на адрес электронной почты подразделения или замещающего лица. | Начальник отдела АСУ |

7 Интернет

Основные нормативные положения по использованию ресурсов сети Интернет приведены в таблице 4.

Таблица 4 - Основные нормативные положения по использованию ресурсов сети Интернет

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
|  | 7.1 Политика получения данных из внешних сетей или через них:  Сетевое оборудование, выполняющее маршрутизацию трафика, должно быть оснащено системой фильтрации трафика с запретительными элементами.  Локальная сеть должна иметь минимальное количество глобальных адресов.  Прокси-сервер должен иметь настроенные умолчанию выключается прямой доступ к сети Интернет с использованием трансляции сетевых адресов.  При необходимости наличия ПК, имеющих прямой выход в сеть Интернет минимизируется число одновременных подключений.  Все компьютеры, находящиеся в сети ЗАО «М-Стандарт» оснащаются антивирусным ПО.  Для всех пользователей запрещается самостоятельная установка нового ПО, в т.ч. полученного из Интернета. |  |
| Доступность изучения информации сети Интернет. | 7.2 Использование ресурсов Интернет доступно с каждого ПК, подключенного в внутренней сети ЗАО «М-Стандарт».  Использование ресурсов сети Internet ограничивается просмотром web-страниц, необходимых в рабочих целях.  Для просмотра web-страниц должны использоваться браузеры, установленные сотрудниками отдела АСУ. Установка и использование других браузеров пользователями запрещается. | Начальник отдела АСУ. |

8 Официальный сайт

8.1 Официальный сайт ЗАО «М-Стандарт» является электронным средством обмена информацией, в т.ч. с заказчиками.

Техническое управление официальным сайтом ЗАО «М-Стандарт» осуществляется назначенным начальником отдела АСУ ответственным сотрудником – администратором сайта ЗАО «М-Стандарт».

8.2 Основные нормативные положения по формированию информации официального сайта приведены в таблице 5.

Таблица 5 - Основные нормативные положения по формированию информации официального сайта

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
| Полнота информации  на официальном сайте в целом. Доступность использования информации заказчиками. | 8.2.1 Структура официального сайта формируется с соблюдением принципов:  - достоверности и актуальности информации;  - охвата информацией всех оказываемых ЗАО «М-Стандарт» услуг и их вариантов;  - охвата для каждой услуги всех практических вопросов, которые необходимы клиенту для получения информации о порядке оказания услуги, стоимости, контактных данных для обращения за услугой, порядка подачи заявок и пр.;  - четкости, однозначности, необходимой краткости и практичности информации об услугах, отсутствия излишних экскурсов, описаний и комментариев;  - возможности получить информацию в рамках публичных оферт;  - наглядности представления информации на страницах;  - наличия возможностей онлайн-связи и взаимодействия, в т.ч. по вопросам получения пояснений, направления заявки и пр.;  - возможностей перехода для получения конкретизированной информации по ссылке при упоминании вида услуги; - регулярность обновления новостной информации;  - наличие блоков актуальной информации рекламного характера, представляемых на заставке сайта и их регулярное обновление;  - возможностей поиска информации по признакам как в рамках сайта в целом, так и в рамках разделов (прейскурант и пр.).  Структура официального сайта должна содержать как минимум:  - сведения о местоположении ЗАО «М-Стандарт»;  - сведения о руководстве ЗАО «М-Стандарт», контактные данные;  - информацию о подразделениях ЗАО «М-Стандарт», их контактную информацию;  - информацию обо всех видах деятельности ЗАО «М-Стандарт», порядке осуществления видов деятельности;  - сведения об аттестатах аккредитации по видам деятельности и содержании областей аккредитации, дипломы, награды;  - сведения о стоимости работ (услуг) ЗАО «М-Стандарт»;  - ресурс обратной связи с заказчиками, предоставляющий заказчикам возможность выражения мнения об уровне оказания услуг, подачи предложения, жалобы, возможности задать вопрос руководству ЗАО «М-Стандарт» и пр. в онлайн-режиме;  - ресурс для размещения анкет и опросов;  - формы типовых договоров на проведение работ (оказание услуг);  - информацию о публичных офертах (при наличии);  - формы заявок на проведение работ;  - ресурс поиска информации в пределах сайта;  - информация о мероприятиях, проводимых ЗАО «М-Стандарт» для заказчиков;  - ресурсы размещения информации об аккредитованных областях деятельности, ведение которых является требованиями нормативных документов, устанавливающих требования к аккредитованным лицам (Орган по сертификации и пр.);  - ресурс размещения новостей деятельности организации, новостей технического регулирования, метрологии оценки соответствия, отдельный ресурс размещения исторической информации и пр. | Главный специалист  (по инновационной деятельности и развитию). |
| Актуальность, достоверность специфической информации | 8.2.2 Перечень ответственности за формирование страниц  Для определения лиц, ответственных за актуализацию специфических видов информации (разделов и страниц сайта, посвященных определенной теме/виду деятельности) формируется перечень ответственности за информацию официального сайта ЗАО «М-Стандарт».  Перечень формируется на основе перечня основных текстов страниц сайта для администратора сайта, для каждого основного текста страницы сайта определяется ответственное лицо и необходимость формирования по данному блоку новостной информации.  Перечень, предварительно согласуется с руководителями подразделений и представителями администрации – внесенными в него в качестве ответственных лиц, утверждается генеральным директором, направляется всем ответственным лицам и в отдел АСУ для настройки автоматических процессов мониторинга. |  |
| Ответственные лица осуществляют мониторинг соответствующей информации на страницах сайта, которые содержат информацию согласно исходным основным текстам страниц не реже одного раза в квартал; для чего ежеквартально в 1С документообороте формируется процесс проведения мониторинга (Исполнение) со ссылками на соответствующие ресурсы сайта согласно закрепленному блоку информации, процесс направляется ответственным лицам согласно перечню. По завершении мониторинга ответственное лицо проставляет отметку о выполнении, при необходимости актуализации создает на основании процесса мониторинга задачу по сайту с приложением предложений по актуализации информации по закрепленному разделу. Мониторинг проводится в течение пяти рабочих дней.  При проведении мониторинга также оценивается наличие информационных поводов для размещения новостей. При наличии информационных поводов - определяют темы и формы публикации новостной информации о деятельности (сообщения, статьи, заявления, информация о выступлениях, фотографии, видеоролики) и направляют в виде задачи по обновлению информации на сайте с приложением новостной информации. | Лица, ответственные за формирование страниц (специфической информации). |
| Согласованная актуализация информации | 8.2.3 Обновление информации на сайте инициируется соответствующим процессом 1 С ЭДО с этапами:  - согласование с главным специалистом (по инновационной деятельности и развитию) - 3 рабочих дня (1 рабочий день для новостной информации);  - размещение администратором официального сайта – 4 рабочих дня (1 рабочий день для новостной информации». | Лица, ответственные за формирование страниц (специфической информации) – своевременное направление информации. |
| Согласованная актуализация информации | При необходимости в рамках согласования главным специалистом (по инновационной деятельности и развитию) может быть направлена дополнительная задача по обработке информации ведущему специалисту по связям с общественностью в целях приведения информации в состояние согласованности и логичности изложения. При внесении существенных изменений – итоговая информация дополнительно согласуется с ответственным за страницу сайта лицом. | Главный специалист (по инновационной деятельности и развитию) - оценка информации.  Начальник отдела АСУ – техническое размещение. |

9 Внутренняя электронная оболочка

9.1 Внутренние электронные данные и документированная информация (информация, содержащаяся на внутренних электронных ресурсах, внутренняя информация)

Основные нормативные положения по использованию внутренних электронных данных и документированной информации приведены в таблице 6.

Таблица 6 - Основные нормативные положения по использованию внутренних электронных данных и документированной информации

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
|  | 9.1.1 Политика контроля доступа:  Сотрудникам ФБУ "М-Стандарт" запрещено осуществление противоправных действий:  - по получению несанкционированного доступа к любой автоматизированной системе;  - по нанесению ущерба и нарушению работы автоматизированных систем;  - по перехвату паролей или иному способу получения паролей, ключевой информации или иных механизмов доступа, которые могут быть использованы для НСД.  ПО, предполагающее использование механизмов разделения доступа или подразумевающее индивидуальную ответственность сотрудника за осуществляемые действия, должно использовать механизм контроля доступа, с идентификацией и авторизацией пользователя с помощью, как минимум пароля, отвечающего требованиям парольной защиты.  Доступ к информации ограниченного доступа должен соответствовать требованиям нормативно-правовых актов РФ, нормативных и организационно-распорядительных документов ЗАО «М-Стандарт», в т.ч. в конкретных областях деятельности.  Формируемые меры безопасности для автоматизированных рабочих мест и компьютерных сетей должны быть просты для использования, управления и аудита.  Настройка доступа ко всем информационным ресурсам должна быть по умолчанию направлена на предотвращение к ним любого несанкционированного доступа.  Если система контроля доступа вышла из строя, то доступ пользователей должен быть запрещен до решения проблемы.  До предоставления прав доступа к информационным ресурсам ФБУ "М-Стандарт", пользователь должен быть ознакомлен под роспись с внутренними нормативными и организационно-распорядительными документами ЗАО «М-Стандарт», регламентирующими работу с конкретными информационными ресурсами.  В случаях, когда это определено необходимостью или требованиями нормативно-правовых актов РФ или внутренних нормативных, организационно-распорядительных документов ЗАО «М-Стандарт» должен быть проведен дополнительный инструктаж или обучение с документированием факта обучения.  В случаях, когда это определено нормативно-правовыми актами РФ или внутренними нормативными, организационно-распорядительными документами ЗАО «М-Стандарт», сотрудник помимо ознакомления, должен письменно подтвердить свое обязательство выполнять требования документов.  Для реализации настоящей Политики в ФБУ «М-Стандарт определяется порядок предоставления доступа и управления доступом с формированием требований безопасности управления доступом, к компьютерным системам, создаются идентификаторы учетных записей и учетные записи специальных типов (СТО 070-006, положения настоящего СТО, организационно - распорядительных документов и пр.) |  |
|  | 9.1.2 Политика защиты данных:  - передача видов внутренней информации, в т.ч. документированной, которая относится к конфиденциальной, осуществляется в соответствии с ПП 070-001;  - информация в электронном виде, относящаяся к персональным данным сотрудников ЗАО «М-Стандарт», должна быть доступна только лицам, определенным в локальном ЗАО «М-Стандарт» о защите персональных данных. |  |
|  | 9.1.3 Политика «чистого стола» и «чистого экрана»:  Политика «чистого стола» и «чистого экрана» формируется в ЗАО «М-Стандарт» с целью минимизации риска неавторизованного доступа, потери или повреждения документов на бумажных носителях, носителей данных и средств обработки информации.  Политика «чистого стола» относится к документам на бумажных носителях и сменным носителям данных.  Политика «чистого экрана» относится к средствам обработки информации.  Политика применяется как во время рабочего дня, так и при внеурочной работе.  Основными положениями настоящей Политики являются:  - для исключения компрометации информации бумажные и съемные электронные носители информации, фотокопировальные устройства, когда они не используются, хранятся в местах вне свободного доступа лиц, не пользующихся данной информацией (под присмотром ответственных лиц или в запирающихся шкафах или помещениях, местах архивного хранения);  - носители с важной или критичной служебной информацией, когда они не требуются, хранятся в сейфах;  - персональные компьютеры и принтеры должны быть выключены по окончании работы;  - в случаях, когда средства доступа к электронной информации (ПК и пр.) находятся без присмотра работающего с ним лица, доступ к информации защищается паролем;  - напечатанные документы с важной или конфиденциальной информацией необходимо изымать из принтеров немедленно. |  |
| Предоставление контролируемого доступа | 9.1.4 Доступ к информационным ресурсам электронного документооборота 1С предоставляется всем сотрудникам ЗАО «М-Стандарт». При принятии нового сотрудника Учреждения – одновременно с ознакомлением с должностной инструкцией сотрудник знакомится под роспись с внутренними нормативными документами, определяющими правила работы в электронном пространстве ЗАО «М-Стандарт» (настоящий документ; документ, определяющий правила управления  документированной информацией, документ, определяющий правила управления персоналом).  Доступ сотрудников к специальным программным ресурсам хранения и обмена информацией (1С Бухгалтерия, ПО «Метрология М-Стандарт» и пр.) осуществляется согласно выполняемым им функциям по служебной записке руководителя подразделения, согласно которой определяется объем доступа и права. Доступ предоставляется в течение трех рабочих дней.  Представителям руководства и администрации ЗАО «М-Стандарт» предоставляются права доступа к программным ресурсам в соответствии со служебной запиской данного сотрудника, согласованной с генеральным директором.  Доступ сотрудников ЗАО «М-Стандарт» в электронные программные ресурсы хранения и обмена информацией (1С Бухгалтерия, ПО «Метрология М-Стандарт» и пр.) осуществляется с использованием средств личной электронной идентификации – логина и пароля.  Средства ЭИ М-Стандарт формируются на основе использования сотрудником закрепленного логина и пароля при входе во внутренние информационные базы данных, работе в используемом в Учреждении ПО, в соответствии с нижеизложенными правилами парольной защиты. Средства ЭП М-Стандарт также могут содержать уникальное визуальное представление, идентифицирующее его с обладателем - сотрудником ЗАО «М-Стандарт» (допускается изображение личной подписи), которое при необходимости может быть выведено при просмотре подписанного документа или записи, его распечатке. Передача сведений о логине и пароле для доступа в ПС ЭДО иным лицам запрещается.  Средства ЭИ М-Стандарт формируются для каждого сотрудника Учреждения, имеющего доступ к работе в сетевых ресурсах, используемом в ЗАО «М-Стандарт» ПО.  Ответственность за надлежащее формирование, хранение передачу средств ЭИ М-Стандарт сотрудникам несет начальник отдела АСУ.  Ответственность за надлежащее использование средств ЭИ М-Стандарт несет каждый сотрудник Учреждения, использующие идентифицированное с ним средство ЭИ М-Стандарт. | Начальник отдела АСУ (руководители подразделений  в рамках предоставления прав). |
| Предоставление контролируемого доступа | 9.1.5 Правила формирования парольной защиты (ЭИ):  1) отдел АСУ является централизованной службой парольной защиты в организации. Задачей данной службы является организационно - техническое обеспечение процессов генерации, смены и удаления паролей во всех автоматизированных системах и ЭВМ сотрудников организации, разработка всех необходимых инструкций и контроль за действиями персонала при работе с использованием паролей;  2) личные пароли должны выбираться пользователями автоматизированной системы самостоятельно в соответствии с требованиями:  - длина пароля должна быть не менее 7 символов;  - в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры или специальные символы (@, #, $, &, \*, % и т.п.);  3) пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP и т.д.);  4) при смене пароля новое значение должно отличаться от предыдущего (не менее, чем двух символах);  5) личный пароль пользователь не имеет права сообщать никому;  6) в случае, если формирование личных паролей пользователей осуществляется отделом АСУ, ответственность за правильность их формирования и распределение возлагается на отдел АСУ;  7) полная плановая смена паролей должна проводиться регулярно, не реже одного раза в три года;  8) внеплановая смена (удаление) личного пароля любого пользователя автоматизированной системы в случае прекращения его полномочий должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой, ответственность возлагается на отдел АСУ;  9) внеплановая полная смена паролей должна производиться в случае прекращения полномочий администраторов информационной безопасности и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной автоматизированной системы, а значит, кроме личного пароля, им могут быть известны пароли других пользователей системы;  10) в случае компрометации личного пароля хотя бы одного пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п. 5 (при необходимости, также п. 6) настоящих требований в зависимости от полномочий владельца скомпрометированного пароля, ответственность возлагается на отдел АСУ;  11) владельцы паролей при ознакомлении с подтверждением ознакомления личной подписью с перечисленными выше требованиями подтверждают их принятие, ответственность за использование паролей, за неразглашение парольной информации. | Пользователи электронных ресурсов. |
|  | 9.1.6 Политика использования криптографического контроля  Деятельность ЗАО «М-Стандарт» со средствами криптографической защиты информации (СКЗИ) должна исключать нарушение законодательства Российской Федерации.  В случае, если предполагаемая деятельность со СКЗИ подразумевает необходимость получения лицензии, ЗАО «М-Стандарт» получает такую лицензию или привлекает для подобной деятельности сторонние организации, имеющие соответствующие лицензии.  При использовании СКЗИ для защиты информации ограниченного доступа данные криптографические средства должны соответствовать требованиям по использованию СКЗИ, в т.ч. в конкретной сфере деятельности.  Установка, настройка и техническое сопровождение СКЗИ должно осуществляться квалифицированными специалистами и не нарушать требования, установленные нормативными документами по использованию СКЗИ и в конкретной сфере деятельности.  Использование, в том числе хранение, СКЗИ должно отвечать требованиям законодательства Российской Федерации. |  |
| Идентификация с использованием электронной цифровой подписи. | В рамках внутренней электронной оболочки (ресурсы 1С, при необходимости – иные программные ресурсы, в т.ч. для осуществления производственной деятельности) реализуется возможность подписания сотрудниками документированной информации (в т.ч. записей) простой электронной подписью, усиленной неквалифицированной электронной подписью (ЭЦП), а также возможность направления подписанных ЭЦП документов контрагентам и иным организациям по электронным каналам связи. Подписание документов электронной подписью обеспечивает однозначную идентификацию подписавшего документ (запись) сотрудника, даты подписания (формирования записи, создания измененной записи).  Данная возможность может быть создана:  - путем подписания владельцем подписи отдельного документа или серии документов при работе в соответствующем ПО или во внешнем ресурсе, предусматривающем подписание документов электронной подписью (простой, усиленной квалифицированной);  - путем доступа пользователей к работе в конкретном ПО, предоставляемом только при подтверждении входа простой электронной подписью и подписания в автоматическим режиме простой электронной подписью всех вносимых в ПО данным пользователем записей;  - путем доступа пользователей к работе в конкретном ПО, предоставляемом только при подтверждении входа ЭЦП и подписания в автоматическом режиме усиленной квалифицированной электронной подписью всех вносимых в ПО данным пользователем записей.  Сертификаты ключа проверки электронной подписи и усиленной квалификационный сертификат электронной подписи выдается аккредитованным удостоверяющим центром в соответствии с Федеральным законом «Об электронной подписи» № 63-ФЗ от 06.04.2011. | Начальник отдела АСУ.  Пользователи СКЗИ. |
| Идентификация с использованием электронной цифровой подписи | Круг лиц, для которых создаются (закупаются) усиленные квалифицированные электронные подписи (ЭЦП) определяется согласно служебным запискам руководителей подразделений и сотрудников администрации генеральному директору, по данным служебным запискам генеральный директор принимает решение, при положительном решении служебная записка с резолюцией направляется начальнику юридического отдела для оформления доверенностей. На основе оформленных доверенностей руководители подразделений (сотрудники администрации) анализируют положения должностных инструкций соответствующих сотрудников на предмет наличия в них положений о праве пользования ЭЦП для подписания ДОКИ в рамках деятельности ЗАО «М-Стандарт», при необходимости актуализируют должностные инструкции, инициируют закупки ЭЦП в рамках Комплексного плана развития и обеспечения деятельности ЗАО «М-Стандарт».  Должностные инструкции сотрудников, использующих ЭЦП для подписания документов в рамках деятельности ЗАО «М-Стандарт», должны содержать соответствующие положения о правах, обязанностях и ответственности сотрудника. | Руководители соответствующих подразделений и представители администрации (инициирование, анализ должностных инструкций, формирование закупок) генеральный директор (принятие решения).  Начальник юридического отдела (оформление и учет доверенностей). |
| Идентификация с использованием электронной цифровой подписи | Передача сотруднику носителя ключа ЭЦП, установка на находящийся на его рабочем месте ПК ключа ЭЦП фиксируется актом приема-передачи с указанием способа передачи признаков ЭЦП, составленным сотрудниками отдела АСУ и подписанным сотрудником-владельцем ЭЦП.  Порядок использования сотрудниками их усиленных квалифицированных электронных подписей, простых электронных подписей определяется внутренними нормативными документами для конкретных видов деятельности.  Ключ ЭЦП может использоваться в виде внешнего электронного носителя информации или быть установлен на ПК и электронном рабочем столе, закрепленном за лицом – владельцем ЭЦП или лицом, доступ к электронному рабочему столу ограничен личным логином и паролем сотрудника, который формируется в соответствии с р. 9.1.5 настоящего СТО. Сотрудник несет ответственность за исключение доступа к доступному под его личным логином и паролем электронному рабочему столу на закрепленном за ним ПК иных лиц.  Использование ЭЦП допускается только сотрудниками – которых идентифицирует ключ и сертификат ЭЦП, передача информации, носителей информации ключей и сертификатов ЭЦП иным лицам запрещается.  Сотруднику запрещается использование не принадлежащих ему носителей ключей или не установленной на идентифицированном его логином и паролем электронном рабочем столе информации ключей.  При отсутствии на рабочем месте сотрудника, у которого на закрепленном за ним ПК установлена ЭЦП – ПК должен быть заблокирован или выключен.  При подписании акта приема-передачи СКЗИ сотрудники проходят инструктаж о порядке их использования.  Приобретение носителей с информацией осуществляется согласно СТО 070-010.  ЗАО «М-Стандарт» использует СКЗИ, приобретаемые у компетентных организаций, при использовании в сферах в соответствии с областью действия Федерального закона «О лицензировании отдельных видов деятельности» № 99-ФЗ от 04.05.2011.  Для предотвращения компроментации СКЗИ в виде квалифицированной подписи (ключей пользователей) отделом АСУ ведется учет выданных ключей, и установленных на ПК ключей (учитываются вид ключа, владелец, сроки действия, места установки).  Журнал учета СКЗИ (в форме ключей, криптографического ПО) ведется отделом АСУ в рамках 1С ЭДО М-Стандарт в соответствии с требованиями СТО 070-006 (учет ключей, учет ПО – идентификация ПО, сроки действия, места установки). | Начальник отдела АСУ.  Пользователи СКЗИ. |
| Идентификация с использованием электронной цифровой подписи | В исключительных случаях по решению генерального директора отдельным приказом может быть введен особый порядок использования ЭЦП генерального директора для конкретных целей. |  |
|  | 9.1.7 Политика использования внутренних сетевых служб:  К обмену информацией внутри электронной информационной сети ЗАО «М-Стандарт» допускаются только сотрудники Учреждения (при необходимости – лица, проходящие практику в Учреждении), в соответствии с установленными для каждого правами доступа.  Межсетевые взаимодействия внутренней сети и сети Интернет защищаются симметричными межсетевыми экранами, настроенными для блокировки запрещенных межсетевых взаимодействий. |  |
|  | 9.1.8 Политика сохранения записей:  Действия, осуществляемые пользователями в сети ЗАО «М-Стандарт» и ПО регистрируются в журналах событий.  Все данные, для которых необходимо хранение, формируются с использованием опций сохранения и систематизации соответствующего ПО. |  |
|  | 9.1.9 Политика резервного копирования:  Резервное копирование информации, размещенной на автоматизированных рабочих местах сотрудников и компьютерах, выполняющих функции сервера компьютерной системы, осуществляется уполномоченным лицом.  Для реализации надлежащего резервного копирования определяется порядок резервного копирования рабочей информации, хранения резервных копий, восстановления документированной информации, в т.ч. резервно копированной (СТО 070-006, И 070-005, положения настоящего СТО, внутренних нормативных документов СМ М-Стандарт для конкретных видов деятельности, организационно-распорядительных документов и пр.). |  |
| Разграниченное хранение и использование информации в электронном виде | 9.1.10 Хранение информации на электронных носителях может осуществляться на жестких дисках компьютеров, съемных носителях информации, в виде серверного хранения.  Для хранения файлы могут быть сжаты в заархивированные файлы и папки.  Хранение информации на жестких дисках персональных компьютеров осуществляется в случаях ее хранения для нужд одного пользователя.  Хранение информации в электронном виде осуществляется преимущественно в виде хранения данных на сетевом диске сервера. Хранение данных на сетевом диске сервера осуществляется как для данных, созданных рамках ПО из Единого реестра российских программ для электронных вычислительных машин и баз данных, так и для данных, созданных в рамках программного обеспечения, разработанного ЗАО «М-Стандарт» или сторонними организациями и применяемого при осуществлении деятельности ЗАО «М-Стандарт». | Начальник отдела АСУ (пользователь в рамках предоставленных прав) |
| Разграниченное хранение и использование информации в электронном виде | 9.1.11 При необходимости хранения и использования информации на съемных носителях по заявкам структурных подразделений отдел АСУ планирует закупки, организует хранение и выдачу таких технических средств. Приобретаемые съемные носители информации должны соответствовать требованиям нормативной документации на соответствующий вид носителя и иметь характеристики (в т.ч. объем сохраняемой информации) согласно запросам подразделений. Руководители подразделений несут ответственность за соблюдение надлежащих условий эксплуатации и хранения съемных носителей информации. | Начальник отдела АСУ (пользователь в рамках предоставленных прав. |
| Разграниченное хранение и использование информации в электронном виде. | 9.1.12 Для разграниченного доступа пользователей на сетевой диск сервера используется диск «W» - осуществляется доступ определенных групп пользователей (разделенных по подразделениям ЗАО «М-Стандарт») к частям сетевого диска «W».  Сетевой диск «Y» является ресурсом общего доступа для пользователей ЗАО «М-Стандарт», информация данного диска не резервируется.  Права доступа к тем или иным серверным ресурсам предоставляются начальником отдела АСУ по заявке руководителей подразделений (в виде служебной записки на имя начальника отдела АСУ) и согласованию при необходимости с генеральным директором или заместителями генерального директора, которым подчиняются соответствующие подразделения. Обеспечение доступа осуществляется в течение трех рабочих дней с момента подачи заявки.  При необходимости разграничение доступа к информации в рамках ПО (как внешнего ПО при наличии соответствующих опций, так и ПО, разработанного ЗАО «М-Стандарт») осуществляется путем ограничения (регулирования) прав доступа идентифицированные пользователей к определенным частям информационных ресурсов ПО (полный запрет доступа, ограничения доступа, в частности для редактирования). | Начальник отдела АСУ (пользователь в рамках предоставленных прав. |
| Разграниченное хранение и использование информации в электронном виде. | 9.1.13 При организации серверного хранения информации должна обеспечиваться отказоустойчивость оборудования, надежность хранения данных и их восстанавливаемость при отказах, наличие защищенного резервного копирования информации (кроме информации на диске «Y»).  Резервное копирование информации в рамках ПО, сетевых дисков «W» осуществляется с шагом не реже одного раза день. Хранение резервных копий осуществляется на отдельном носителе с соблюдением условий окружающей среды согласно технической документации.  Резервные копии документированной информации формируются в нередактируемом формате, ресурс хранения резервных копий должен обеспечивать полную идентичность резервной копии и скопированной информации, создаваться с возможностью поиска информации по идентификационным признакам (например, дата, источник, вид информации и пр.).  Также положения настоящего раздела и Политик в части резервного копирования и восстановления информации распространяются на документированную информацию в электронном виде, сформированную для резервного копирования и восстанавливаемости созданных на бумажных носителях документов (скан-копии бумажных документов), размещаемых в ресурсах ПО (1С ЭДО М-Стандарт, разработанного ЗАО «М-Стандарт» ПО). | Начальник отдела АСУ (пользователь в рамках предоставленных прав). |
| Разграниченное хранение и использование информации в электронном виде. | 9.1.14 К средствам внутренней электронной информационной среды относятся:  - содержащие справочную информацию внутренние информационно-справочные ресурсы - сетевой ресурс «Y» / «Справочная»;  - внутренний информационный портал ЗАО «М-Стандарт»;  - справочные ресурсы ПС ЭДО 1С;  - внутренние ресурсы обмена информацией - диск «Y» / «Обменник» для передачи подразделениям ЗАО «М-Стандарт» в электронном виде, используемая для обмена сообщениями программа электронной почты;  - опция постановки задач ПС 1С ЭДО. | Начальник отдела АСУ (пользователь в рамках предоставленных прав. |
| Разграниченное хранение и использование информации в электронном виде. | 9.1.15 Информация, предназначенная для обмена между подразделениями ЗАО «М-Стандарт» размещается в ресурсе «Обменник» в папках с обозначениями подразделений, размещающих информацию для обмена. Файлы из ресурса «Обменник» могут быть скопированы всеми пользователями сети ЗАО «М-Стандарт», запрет для редактирования не устанавливается.  К размещению и удалению информации в папке соответствующего подразделения имеют допуск пользователи всех подразделения.  Информация, размещаемая в ресурсе «Обменник» может находиться там три месяца. Файлы и папки, размещенные в ресурсе «ОБМЕННИК» и хранящиеся там более трех месяцев могут быть удалены администратором при необходимости оптимизации данных. | Начальник отдела АСУ (пользователь в рамках предоставленных прав. |
| Разграниченное хранение и использование информации в электронном виде. | 9.1.12 Электронное средство внутреннего информационного портала ЗАО «М-Стандарт» формируется отделом АСУ в качестве заставки при входе пользователя в сеть Интернет.  Внутренний информационный портал содержит:  а) контактную информацию сотрудников ЗАО «М-Стандарт»;  б) опцию прямого обращения и генеральному директору, к ответственным лицам ЗАО «М-Стандарт» по решению социальных вопросов (ДМС и пр.);  в) информацию об актуализации внутренних электронных ресурсов ПО ЗАО «М-Стандарт»;  г) ссылки на актуальные внешние электронные ресурсы;  д) информацию о планируемых мероприятиях;  е) опции обращения в технические службы ЗАО «М-Стандарт» с автоматической постановкой задач 1С Документооборот М-Стандарт»;  ж) иную внутреннюю новостную информацию и объявления (состав информации определяется в рабочем порядке в соответствии с актуальными необходимостями).  Размещение информации на внутреннем информационном портале ЗАО «М-Стандарт» осуществляется путем размещения информации сотрудником отдела АСУ, в т.ч. полученной соответствующей задачи ПС ЭДО 1С от ответственного лица за ведение портала в течение одного рабочего дня с момента получения.  Ответственность за размещение и актуальность данных а) – г) внутреннего информационного портала ЗАО «М-Стандарт» несет начальник отдела АСУ.  Определение состава новостной информации, ответственность за размещение и актуальность данных д) – е) внутреннего информационного портала ЗАО «М-Стандарт» несет главный специалист (по инновационной деятельности и развитию. | Начальник отдела АСУ (пользователь в рамках предоставленных прав. |

9.2 Размещение информационных материалов во внутренних справочных электронных ресурсах ЗАО «М-Стандарт»

Сведения о местах размещения и ответственных за размещение информационных материалов во внутренней электронной оболочке приведены в таблице 7.

Указанная в таблице 7 информация на диске «Y» / «Справочная» размещается в папках ограниченного доступа (доступ для редактирования лиц руководителей или назначенных сотрудников подразделений согласно таблиц). Документы, действие которых отменено, помещаются в справочных целях в папки соответствующих ресурсов, обозначенные «Отменные документы справочно» и пр.

Таблица 7 - Сведения о местах размещения и ответственных за размещение информационных материалов во внутренней электронной оболочке.

|  |  |  |  |
| --- | --- | --- | --- |
| Размещаемый материал | Срок размещения | Ответственный за размещение | Информационно-справочный ресурс размещения |
| Комплексный план развития и обеспечения деятельности ЗАО «М-Стандарт» и изменения. | Не позднее десяти рабочих дней после утверждения плана и изменений. | ПЭО. | Диск Y / Отделы / 1402.  ПО 1С Бухгалтерия М-Стандарт / Закупки. |
| Положение об оплате труда работников ЗАО «М-Стандарт». | Не позднее десяти рабочих дней после утверждения положения и изменений. | ПЭО. | Диск Y / Отделы /1402.  1С Документооборот М-Стандарт (в рамках процесса ознакомления с утверждающим приказом, формируется ОУП). |
| Прейскурант цен на работы (услуги) ЗАО «М-Стандарт». | Не позднее десяти рабочих дней после утверждения прейскуранта и изменений. |  | Диск Y / Отделы / 1402.  1С Документооборот М-Стандарт (в рамках процесса ознакомления с утверждающим приказом, формируется ОУП). |
| Локальные акты ЗАО «М-Стандарт» по кадровым вопросам. | В течение пяти рабочих дней после принятия. | ОУП. | 1С Документооборот М-Стандарт (доступность в соответствии со списками ознакомления). |
| Организационно-распорядительные документы ЗАО «М-Стандарт». | В течение трех рабочих дней после утверждения. | Служба режима и делопроизводства ОУП. | 1С Документооборот М-Стандарт (доступность в соответствии со списками ознакомления). |
| Копии правоустанавливающих и регистрационных документов ЗАО «М-Стандарт» (Устав, свидетельство о постановке на учет в налоговых органах, свидетельство о внесении в единый реестр юридических лиц и пр.). | В течение пяти рабочих дней после получения. | Начальник юридического отдела. | Диск Y /Отделы / Юрист. |
| Типовые формы документов в области гражданско-правовых и трудовых отношений (договоры, контракты, соглашения и пр.). | В течение пяти рабочих дней после принятия согласно СТО 070-009. |  | 1С Документооборот М-Стандарт / Документы внутренние / 1700 / Типовые договоры и Диск Y / Справочная / Типовые договоры. |
| Внутренние документы в области охраны труда и промышленной безопасности. | В течение пяти рабочих дней после принятия. | Специалист по охране труда 1 категории. | Диск Y / Справочная / Охрана труда. |
| Нормативные, методические документы и материалы по гражданской обороне. | В течение пяти рабочих дней после принятия или получения. | Сотрудник ЭТО, ответственный за ГО и ЧС. | Диск Y / Справочная / Гражданская оборона. |
| Формы документов по аттестации эталонов. | В течение пяти рабочих дней после принятия или получения. | Отдел метрологического обеспечения, стандартизации и экспертных работ. | Диск Y / Справочная/ Формы аттестации эталонов.  1С Документооборот М-Стандарт. |
| Актуальная карточка предприятия. | В течение двух рабочих дней после внесения изменений. | Бухгалтерия | Диск Y / Справочная / Бухгалтерия. |
| Положение о командировках ЗАО «М-Стандарт». | В течение пяти рабочих дней после принятия или внесения изменений |
| Коллективный договор. | В течение пяти рабочих дней после принятия или внесения изменений. | Юридический отдел. | Диск Y / Справочная / Коллективный договор. |
| Перечни документов системы менеджмента ЗАО «М-Стандарт» в области обеспечения качества работ (услуг), системы менеджмента качества по обеспечению единства измерений.  Документы системы менеджмента ЗАО «М-Стандарт» в области обеспечения качества работ (услуг).  Политики и заявления руководства ЗАО «М-Стандарт» в области качества.  Документы по результатам внутренних аудитов ФБУ  «М-Стандарт».  Проекты документов, доступные для обсуждения. | В течение пяти рабочих дней после принятия или внесения изменений.  Проверка актуальности не реже одного раза в месяц. | Главный специалист (по качеству). | Диск Y / Справочная/система менеджмента.  1С Документооборот М-Стандарт. |
| Копии сертификатов, аттестатов, свидетельств, лицензий, областей аккредитации и иных документов о признании и подтверждении соответствия по вопросам деятельности ЗАО «М-Стандарт». | В течение четырех рабочих дней после получения оригиналов. | Главный специалист (по качеству). | Диск Y / Справочная/система менеджмента.  1С Документооборот М-Стандарт. |

9.3 Удаленный доступ

Основные нормативные положения по использованию удаленного доступа приведены в таблице 8.

Таблица 8 - Основные нормативные положения по использованию удаленного доступа

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
|  | 9.3.1 Политика дистанционной работы (мобильной обработки данных):  Сотрудникам ЗАО «М-Стандарт» в рамках производственных необходимостей предоставляется возможность доступа в сетевые ресурсы и ПО ЗАО «М-Стандарт» с мобильных устройств (мобильный доступ ЗАО «М-Стандарт»).  Мобильный доступ предоставляется с использованием лицензированного ПО, мобильных устройств, контролируемых ЗАО «М-Стандарт», контролируемых каналов связи.  Отделом АСУ ведется контроль состояния, учет пользователей и устройств мобильного доступа.  Запрещается использование мобильного доступа с устройств и с использованием ПО, не учтенных отделом АСУ. |  |
| Надлежащее управление данными при удаленном доступе. | 9.3.2 В соответствии со служебными записками руководителей, сотрудников администрации, направляемыми начальнику отдела АСУ – сотрудникам ЗАО «М-Стандарт» предоставляется доступ к работе в электронной оболочке (включая ПО), с мобильных ПК и устройств при нахождении вне производственных помещений ЗАО «М-Стандарт» (мобильный доступ).  При предоставлении мобильного доступа формируется отдельный логин и пароль.  Начальником отдела АСУ организуется учет предоставленного мобильного доступа в форме электронных записей (1С) с указанием сотрудника, объема предоставленного доступа (ресурсов, к которым предоставлен доступ, прав). | Начальник отдела АСУ. |

10 Программные средства

Основные нормативные положения по формированию и использованию программных средств приведены в таблице 9.

Таблица 9 - Основные нормативные положения по формированию и использованию программных средств

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
|  | 10.1 Политика разрешенного/неразрешенного программного обеспечения:  ПО, в рамках которого осуществляется сбор, обработки, регистрация, хранение информации, должно обеспечивать серверное хранение данных и документов.  ПО, используемое для осуществления деятельности структурных подразделений, должно соответствовать условиям его лицензирования (независимо от того, является ли оно коммерческим или свободно распространяемым) и использоваться строго в соответствии с лицензионным соглашением.  Любое подразделение ЗАО «М-Стандарт» должно исключить случаи хранения и использования ПО, не являющегося лицензионным.  В случае если в нормативно - правовыми актами РФ предъявляются особые требования к ПО (например, требование по сертификации такого ПО уполномоченными организациям и т.п.) - подразделение осуществляет закупку или инициирует разработку ПО с выполнением таких требований. |  |
| На каждое автоматизированном рабочем месте должен быть установлен комплект ПО, необходимый и достаточный для выполнения на нем поставленных задач.  Отдел АСУ предоставляет сотрудникам достаточное количество лицензий на использование ПО, необходимого для выполнения должностных обязанностей.  На технические средства, подключаемые к компьютерной сети и подразумевающие возможность установки прикладного ПО, должно быть установлено базовое ПО, предусмотренное «Реестром программного обеспечения» и предназначенное к установке на технических средствах, подключаемых к компьютерной сети».  Обновление версий ПО, использующего ресурсы компьютерных сетей, должно осуществляться только сотрудниками отдела АСУ или их привлечением. Допустимо использование функции автоматического обновления ПО, использующего ресурсы компьютерной сети.  Удаление любого ПО должно производиться сотрудниками отдела АСУ. |
| Обеспечение производственных нужд программным обеспечением, обеспечивающим надлежащую обработку, хранение информации в соответствии с конкретной задачей. | 10.4 Обработка данных в электронном виде осуществляется путем использования программного обеспечения или соответствующих приложений ПО из Единого реестра российских программ для электронных вычислительных машин и баз данных.  Для управления электронной обработкой данных может использоваться программное обеспечение внешних разработчиков, приобретенное в соответствии с СТО 070-010 и программное обеспечение, разработанное ЗАО «М-Стандарт».  Запрос на установку ПО формируется сотрудником подразделения, для работ которого данное ПО необходимо, посредством опции подачи заявок в отдел АСУ ПО 1С ЭДО (установка программного обеспечения – метрологическое или иное ПО), инициатор в рамках заявки предоставляет необходимые сведения о ПО. Заявка согласуется начальником отдела АСУ, выполняется ответственными сотрудниками отдела АСУ. При необходимости закупки приобретение программного обеспечения внешних разработчиков осуществляется в плановом или внеплановом порядке согласно СТО 070-010. | Инициатор ПО.  Начальник отдела АСУ. |
| 10.5 Разработка, модернизация и актуализация программного обеспечения проводится при возникновении производственной необходимости в подразделениях ЗАО «М-Стандарт».  Для разработки, модернизации и актуализации программного обеспечения руководитель структурного подразделения или лицо, назначенное руководством ЗАО «М-Стандарт» ответственным за управление ПО по конкретному вопросу (инициатор ПО), формирует запрос на разработку/модернизацию ПО с изложением исходной технической информации для разработки. Запрос направляется в виде служебной записки начальнику отдела АСУ. При необходимости начальник отдела АСУ и лицо, направившее запрос дополнительно согласуют формирование ПО с генеральным директором. |
| Обеспечение производственных нужд программным обеспечением, обеспечивающим надлежащую обработку, хранение информации в соответствии с конкретной задачей. | При получении запроса начальник отдела АСУ организует составление технического задания на разработку ПО, которое согласуется с лицом, направившим запрос, после чего задача 1С ЭДО по созданию/модернизации ПО направляется для исполнения сотруднику отдела АСУ.  Сроки разработки в дальнейшем согласуются с начальником отдела АСУ, при необходимости корректируются и согласуются положения технического задания. После согласования сроков и вида ПО, начальник отдела АСУ организует разработку в установленные сроки. При возникновении разногласий руководители подразделений и отдела АСУ обращаются к генеральному директору ЗАО «М-Стандарт» или заместителю генерального директора для решения вопросов о необходимости и сроках разработки, что может быть в дальнейшем оформлено организационно-распорядительными документами согласно СТО 070-006.  Техническое задание (исходную техническую информацию) на разработку, модернизацию и актуализацию программного обеспечения формируется с учетом требований к представлению исходных данных для разработки ГОСТ 34.602, ГОСТ 19.201 и должно содержать необходимую для разработки (модернизации, актуализации) ПО сотрудником отдела АСУ исходную информацию:  - цель создания (модернизации, актуализации) ПО;  - вид и размер вводимых данных;  - необходимые характеристики преобразования данных в рамках ПО (в т.ч. формулы);  - вид и размер преобразованных данных;  - направления движения данных;  - образцы (формы) наглядной информации (в т.ч. документов), создаваемых с помощью данного ПО (при необходимости);  - иную информацию, необходимую для создания (модернизации, актуализации) конкретного ПО.  Разработка ПО может осуществляться в плановом порядке путем включения положений в Комплексный план развития и обеспечения деятельности ЗАО «М-Стандарт» согласно СТО 070-010, а также иные документы о планировании. | Инициатор ПО.  Начальник отдела АСУ. |
| Обеспечение производственных нужд программным обеспечением, обеспечивающим надлежащую обработку, хранение информации в соответствии с конкретной задачей. | 10.6 Программное обеспечение, предназначенное для сбора, обработки, регистрации, хранения или поиска данных при проведении испытаний, метрологического подтверждения пригодности должно быть оценено как пригодное для решения конкретных задач.  ПО, приобретенное в комплекте с оборудованием, с документом, подтверждающим его назначение для выполнения конкретных задач (сертификат, свидетельство, обязательство разработчика и пр.) считается достаточно оцененным. Приложения ПО из Единого реестра российских программ для электронных вычислительных машин и баз данных, используемые для сбора, обработки, регистрации, хранения или поиска данных при проведении испытаний, метрологического подтверждения пригодности также считаются достаточно оцененными. |
| Обеспечение производственных нужд программным обеспечением, обеспечивающим надлежащую обработку, хранение информации в соответствии с конкретной задачей. | Программное обеспечение, разработанное ЗАО «М-Стандарт» для сбора, обработки, регистрации, хранения или поиска данных при проведении испытаний, метрологического подтверждения пригодности оценивается специалистами подразделения (подразделений) ЗАО «М-Стандарт» - заказчиками конкретного ПО. Оценка проводится коллегиально комиссией, состоящей из 2-5 сотрудников, деятельность которых предусматривает использование данного ПО. По результатам оценки ПО оформляется протокол оценки, который должен содержать:  - период проведения оценки;  - сведения о лицах, проводивших оценку;  - методику проведения оценки (формируется специалистами, проводящими оценку, в зависимости от задач использования конкретного ПО);  - результаты оценки; - выводы по результатам оценки;  - подписи лиц, проводивших оценку.  При неудовлетворительных результатах оценки ПО возвращается на доработку в отдел АСУ. | Инициатор ПО.  Начальник отдела АСУ. |

11 Учет, техническое обслуживание, проверка

Все технические средства обработки, хранения, воспроизведения информации, используемые в ЗАО «М-Стандарт» (включая ПО), проходят учет, техническое обслуживание, при необходимости – технические проверки.

Основные нормативные положения по учеты, обслуживанию, проверкам электронных средств приведены в таблице 10.

Таблица 10 - Основные нормативные положения по учеты, обслуживанию, проверкам электронных средств

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
| Бесперебойное функционирование электронных технических средств | 11.1 Приобретение электронных средств передачи, хранения и воспроизведения информации, расходных материалов и запасных частей к ним организуются в плановом или внеплановом порядке согласно СТО 070-010 по запросам руководителей подразделений, администрации. Отклонения характеристик технических средств от запрошенных должны быть согласованы с руководителями подразделений-заказчиков до начала процесса их приобретения. | Начальник отдела АСУ. |
| 11.2 Учет электронных технических средств осуществляется в форме электронных учетных записей (в рамках ПО 1С), содержащих сведения:  идентификация электронного технического средства и назначение (наименование, тип, марка, учетный номер изготовителя, иные идентификационные данные, в т.ч. назначение при необходимости);  место использования;  сведения о проведенном техническом обслуживании;  сведения о неисправностях, ремонтах;  сведения о модернизации. |
| Бесперебойное функционирование электронных технических средств | 11.3 Сбои и неполадки в работе ПО подразделяются на:  малозначительные – ПО работает, но существуют отдельные моменты, затрудняющие его эксплуатацию (расположение кнопки или окна);  значительные – ПО в целом работает, но исполнение часть функций не осуществляется;  критические или недопустимые – ПО не может осуществлять свою работу вследствие внутренней ошибки.  Устранение сбоев и неполадок в работе ПО должно осуществляться в максимально короткие сроки, в т.ч. в зависимости от значительности - критические и значительные неполадки при наличии технической возможности должны устраняться в течение одного-трех рабочих дней.  При необходимости для ПО, приобретенного у внешних разработчиков, создаются документы в области гражданско-правовых отношений (договоры, соглашения и пр.), предусматривающие обслуживание ПО. Данные документы должны предусматривать при необходимости возможность оперативного проведения обслуживания и устранения сбоев неполадок. | Начальник отдела АСУ. |
| Бесперебойное функционирование электронных технических средств | 11.4 Техническое обслуживание, устранение неполадок и ремонт электронных средств передачи, хранения и воспроизведения информации, обеспечение расходными материалами осуществляет отдел АСУ, в т.ч. в соответствии с указаниями технической документации оргтехники. При необходимости к проведению данных работ могут быть привлечены сторонние организации в порядке согласно СТО 070-010.  Обслуживание и ремонт электронных средств передачи, хранения и воспроизведения информации, контроль и учет данных работ осуществляется по заявкам сотрудников ЗАО «М-Стандарт» в рамках 1С ЭДО М-Стандарт (опция заявок в отдел АСУ, хранение информации по заявкам и вопросам выполнения осуществляется в рамках папки внутренних документов отдел 1800). Информация о видах подаваемых в отдел АСУ заявок на обслуживание и ремонт в рамках 1С ЭДО М-Стандарт размещается начальником отдела АСУ в справочном ресурсе данной опции.  Заявки сотрудников ЗАО «М-Стандарт», не связанные с ремонтом технических средств, направляются ответственным сотрудникам АСУ для исполнения, по результатам выполнения пользователи проставляют отметку о контроле выполнения.  Заявки сотрудников ЗАО «М-Стандарт», связанные с ремонтом технических средств, дополнительно согласуются с начальником отдела АСУ и руководителями соответствующих подразделений в части необходимости диагностики, проведения ремонта в сторонних организациях, стоимости ремонта. После всех согласований проводится соответствующая закупка согласно СТО 070-010.  Заявки сотрудников ЗАО «М-Стандарт», связанные с выдачей материальных средств для эксплуатации электронных средств передачи, хранения и воспроизведения информации, согласуются с начальником отдела АСУ и руководителями соответствующих подразделений, после согласования ответственным сотрудникам отдела АСУ направляются задачи по выдаче соответствующих материальных средств.  Для замены расходных материалов отдел АСУ создает обменный фонд по типам используемых в подразделениях технических средств. | Начальник отдела АСУ.  Пользователи (в рамках надлежащего использования электронных средств,  направления заявок о контроль исполнения).  Руководители подразделений-пользователей (согласование ремонтных работ). |
| Бесперебойное функционирование электронных технических средств. | При отсутствии расходных материалов для замены сотрудники отдела АСУ производят установку или доступ к пользованию аналогичным технического средства до получения необходимых расходных материалов.  При возникновении неполадок в работе технических и программных средств сотрудники отдела АСУ проводят осмотр техники, диагностику неполадок. Мелкий ремонт и обслуживание проводится на месте сотрудниками отдела АСУ, при необходимости техническое средство ремонтируется и обслуживается в отделе АСУ.  При необходимости проведения работ по техническому обслуживанию и ремонту технических средств с изъятием средства с места эксплуатации более, чем на три рабочих дня при наличии в распоряжении отдела АСУ соответствующего технического средства может быть произведена замена данного технического средства на аналогичное по согласованию между начальником отдела АСУ и руководителем структурного подразделения. | Начальник отдела АСУ.  Пользователи (в рамках надлежащего использования электронных средств,  направления заявок о контроль исполнения).  Руководители подразделений-пользователей (согласование ремонтных работ). |
| Бесперебойное функционирование электронных технических средств | 11.5 Сведения о возможных неполадках оргтехники и рекомендации по обращению с расходными материалами для пользователей  Неполадки в работе печатающих устройств, неисправности картриджей:  - аппарат плохо захватывает бумагу или захватывает сразу несколько листов;  - при печати бумага застревает или заминается;  - происходит несанкционированная остановка печати;  - наблюдается повтор изображения на листе (фантомная печать);  - наблюдается черная полоса на краю листа;  - на листе присутствуют белые либо черные полосы, черные точки;  - при печати вместо текста или изображения из аппарата выходит черный либо белый лист;  - аппарат скрипит, шуршит и пр.  Сведения по использованию и хранению заправленных картриджей:  - картридж чувствителен к механическим повреждениям;  - картридж боится сырости;  - картридж необходимо держать подальше от источников тепла (батареи и пр.);  - при использовании бумаги с печатным материалом на оборотной стороне («обороток») необходимо удалять скрепки и скобки;  - перед установкой картриджа его необходимо встряхнуть;  - нельзя касаться поверхности «фотобарабана» картриджа руками;  - покрытие «фотобарабана» разрушается при попадании на него света, поэтому картридж следует хранить в темном пакете, если он находится вне печатающего устройства;  - при неисправности картридж нельзя разбирать. | Пользователи. |

12 Система менеджмента информационной безопасности

Основные положения о функционировании системы менеджмента информационной безопасности приведены в таблице 11.

Таблица 11 - Основные положения о функционировании системы менеджмента информационной безопасности

|  |  |  |
| --- | --- | --- |
| Решаемая задача | Действия/требования | Ответственный |
| Систематизация обеспечения надлежащего уровня информационной безопасности | 12.1 Обеспечение надлежащего уровня информационной безопасности для электронной информационной среды ЗАО «М-Стандарт» реализуется путем разработки, внедрения и функционирования системы менеджмента информационной безопасности, формируемой руководствуясь основными применимыми положениями ГОСТ Р ИСО/МЭК 27001-2006. СМИБ ЗАО «М-Стандарт» интегрирована с СМ М-Стандарт, ее элементы реализуются в рамках соответствующих элементов СМ М-Стандарт.  Управление ИБ, мониторинг осуществляется в рамках управления процессом поддержания в надлежащем состоянии инфраструктуры и производственной среды, управление рисками в рамках СМИБ осуществляется в соответствии с СТО 070-001, МИ 070-001 в рамках анализа рисков процесса данного процесса.  Внутренние аудиты СМИБ осуществляется в рамках внутренних аудитов СМ М-Стандарт в соответствии с СТО 070-004 в качестве элементов проверок.  Управление несоответствиями в рамках СМИБ (в т.ч. корректирующие действия) реализуется в соответствии с СТО 070-003.  Управление ресурсами в рамках СМИБ осуществляется в порядке согласно СТО 070-005, СТО 070-010.  Оценка и анализ СМИБ, реализация концепции улучшения проводятся в рамках анализа СМ М-Стандарт в соответствии с СТО 070-001.  Управление документацией и записями СМИБ осуществляется в соответствии с положениями СТО 070-006.  12.2 В рамках определения основных положений СМИБ руководством ЗАО «М-Стандарт» принята следующая Политика менеджмента информационной безопасности (Политика СМИБ):  а) Основные цели формирования системы менеджмента информационной безопасности:  - поддержание на приемлемом уровне рисков информационной безопасности;  - защита конфиденциальности информации ЗАО «М-Стандарт» и клиентов;  - сохранение целостности всех данных, в т.ч. учетных;  - соответствие информационных сервисов стандартам доступности;  б) Основные принципы менеджмента информационной безопасности:  - соответствие состояния информационной безопасности и процедур ее осуществления законодательству Российской Федерации  - защищенность информации независимо от ее формы и способа ее распространения, передачи и хранения;  - идентификация рисков информационной безопасности и управление ими (минимизация);  - осведомленность и подотчетность персонала за информационную безопасность;  - достаточность финансирования средств управления информационной безопасностью;  - возможности мошенничества и злоупотреблений в области информационных систем должны быть приняты в расчет при общем управлении информационными системами;  - доступность отчетной информации о состоянии информационной безопасности;  д) Результаты функционирования СМИБ:  - инциденты информационной безопасности не должны приводить к серьезным непредвиденным затратам или серьезным срывам работы служб и деятельности предприятия;  - минимальный объем потерь вследствие недобросовестного использования информации;  - состояние информационной безопасности обеспечивает надлежащий уровень качества услуг, оказываемых клиентам.  Вышеизложенную Политику СМИБ поддерживают частные Политики по конкретным вопросам информационного безопасности, изложенные в настоящем документе и обязательные для руководства в соответствующей деятельности для персонала ЗАО «М-Стандарт». | Генеральный директор – определение политики, организация СМИБ.  Начальник отдела АСУ (технические аспекты и нормы, техническое внедрение и поддержание средств информационной безопасности, консультационная поддержка персонала).  Главный специалист (по качеству) – документирование.  Руководители, представители руководства (организация работы персонала с соблюдением требований к защите информации).  Каждый сотрудник ЗАО «М-Стандарт» (соблюдение положений информационной безопасности при  Выполнении своих должностных обязанностей). |