Акционерное общество «Северсталь Менеджмент»

ПРИКАЗ

10 . 06 . 2026 г. № П-ОД-700-00-26-14

г. Москва

Об утверждении Инструкции пользователя корпоративной информационной системы группы компании «Северсталь»

В целях упорядочивания работы пользователей и повышение уровня безопасности информации при ее обработке с помощью вычислительных средств

ПРИКАЗЫВАЮ:

1. Утвердить и ввести в действие с момента издания настоящего приказа Инструкцию пользователя корпоративной информационной системы группы компаний «Северсталь» (далее - Инструкция) (приложение).

2. Считать утратившим силу с момента издания настоящего приказа Инструкцию, утвержденную приказом генерального директора от 30.10.2014 г. № П-14-0000043.

3. Руководителям функциональных дирекций АО «Северсталь Менеджмент», филиалов, обособленных подразделений и управляемых обществ организовать контроль ознакомления работников с Инструкцией через Личный кабинет HR.

4. Руководителям обществ, не находящихся под управлением АО «Северсталь Менеджмент» и использующих информационные ресурсы корпоративной информационной системы группы компаний «Северсталь», в течение 30 дней с момента издания настоящего приказа своими приказами распространить действие Инструкции на общества.

5. Контроль исполнения настоящего приказа возложить на заместителя директора по информационной безопасности – начальника управления Гусева С. Б.

Генеральный директор А. А. Шевелев

Приложение
к приказу генерального директора
АО «Северсталь Менеджмент»
от 10 06 2026 г. № П-ОД-700-00-26-14

Инструкция
пользователя корпоративной информационной системы
группы компаний «Северсталь»

г. Москва
2026

ОГЛАВЛЕНИЕ

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

Наименование документа:	*Инструкция пользователя корпоративной информационной системы группы компаний «Северсталь»*
Номер документа:	
Версия	2 .
Утверждено	*Приказом Генерального директора АО «Северсталь Менеджмент»* №П-ОД-700-00-26-14 *от* 10.06.2026 г.
Дата введения в действие	10.06.2026 г.
Дата пересмотра	10.06.2031 г.
Подразделение - разработчик	Управление информационной безопасности

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая Инструкция определяет обязанности, ответственность и полномочия работников АО «Северсталь Менеджмент» (включая филиалы и обособленные подразделения), управляемых обществ и их дочерних компаний, иных предприятий, входящих в группу компаний «Северсталь» (далее - Общества), и сторонних организаций, работающих с корпоративной информационной системой, оборудованием, программным обеспечением и информационными ресурсами Общества.

1.2. Целью настоящей Инструкции является информирование, упорядочивание работы пользователей и повышение уровня безопасности информации при ее обработке с помощью вычислительных средств.

1.3. Все технические, программные и информационные ресурсы, входящие в корпоративную информационную систему, являются собственностью Общества.

1.4. Настоящая Инструкция утверждается генеральным директором АО «Северсталь Менеджмент».

1.5. На предприятиях, не находящихся под управлением АО «Северсталь Менеджмент», Инструкция вводится в действие приказом руководителя соответствующего предприятия.

2. НОРМАТИВНЫЕ ССЫЛКИ

2.1. Стандарт группы компаний «Северсталь» «Информационная безопасность».

2.2. Положение по управлению доступом к информационным ресурсам группы компаний «Северсталь».

2.3. Политика парольной защиты группы компаний «Северсталь».

2.4. Политика АО «Северсталь Менеджмент» в области защиты информации.

2.5. Стандарт поведения работников группы компании «Северсталь».

2.6. Инструкция по самостоятельному обновлению баз антивируса

2.7. Программное обеспечение, запрещенное к использованию

2.8. Положение по использованию публичных и корпоративных социальных медиа и мессенджеров

3. ОСНОВНЫЕ СОКРАЩЕНИЯ

Принятое сокращение	Полное наименование
ИБ	Информационная безопасность
КИС	Корпоративная информационная система
КСПД	Корпоративная сеть передачи данных
ПО	Программное обеспечение
РС	Рабочая станция
СВТ	Средство вычислительной техники
УИБ	Управление информационной безопасности АО «Северсталь Менеджмент»
VPN	Virtual Private Network (виртуальная частная сеть)

4. ОСНОВНЫЕ ТЕРМИНЫ

Зарегистрированный съемный носитель информации	Съемный носитель информации, принадлежащий работодателю и выданный работнику Общества по заявке.
Защита информации	Комплекс мер, направленных на обеспечение конфиденциальности, целостности и доступности данных. Включает технические, организационные и правовые меры, которые минимизируют риски утечки, повреждения или несанкционированного доступа к информации.
Информация, подлежащая защите (защищаемая информация)	Информация, составляющая коммерческую тайну, определенная Перечнем информации, составляющей коммерческую тайну Общества, персональные данные, определенные Перечнем персональных данных, обрабатываемых в Обществе, иная охраняемая законом информация и сведения ограниченного доступа.
Информационный ресурс	Предметно-ориентированный элемент информационной системы, использующийся в модели разграничения доступа информационной системы как объект доступа.
Корпоративная информационная система	Совокупность находящейся в электронном виде информации и обеспечивающих ее обработку информационных технологий и технических средств (в т. ч. КСПД), используемых на предприятиях группы компаний Северсталь.
Корпоративная сеть передачи данных	Телекоммуникационная сеть, объединяющая в единое информационное пространство все структурные подразделения

	Общества и обеспечивающая одновременную передачу данных, взаимодействие приложений, расположенных в различных узлах, доступ к ним пользователей.
Корпоративное ИТ-подразделение	Работники Общества, в обязанности которых входит обработка обращений пользователей по восстановлению ИТ-сервисов, оказание консультаций по вопросам использования КИС и предоставления ИТ-сервисов, а также работники, обеспечивающие сопровождение и обслуживание СВТ.
Мобильный компьютер	Переносное средство вычислительной техники (ноутбук, планшет, промышленный мобильный терминал и т.п.).
Пользователь	Физическое лицо, имеющее доступ к ресурсам корпоративной информационной системы Общества посредством вычислительной техники.
ПО для организации защищенных каналов VPN, сторонние VPN-сервисы и прочие сервисы проксирования трафика.	Специализированное программное обеспечение, средства и инфраструктура, используемые для скрытого или косвенного сетевого взаимодействия с ресурсами Интернет с целью сокрытия реального местоположения и идентификации пользователя, обхода блокировок сайтов и локальных ограничений.
Рабочая станция	Стационарный или мобильный компьютер, предоставленный Обществом пользователю для выполнения служебных обязанностей.
Работник УИБ	Работник Общества, в должностные обязанности которого входит организация системы управления информационной безопасностью и обеспечение ее функционирования
Средство вычислительной техники	Совокупность программных и технических элементов систем обработки данных Общества, способных функционировать самостоятельно или в составе других систем.
Съемный носитель информации	Переносное устройство хранения информации, выполненное в форме съемного внешнего диска, USB брелока, USB-бокса, смарт-карты, а также кард-ридеры, оптические диски и т.п., временно подключаемые к рабочим станциям и другим устройствам.

5. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ

5.1. Общие обязанности

5.1.1. Соблюдать требования настоящей Инструкции при работе с информационными ресурсами Общества.

5.1.2. Аккуратно обращаться с выданным оборудованием и информацией, обеспечивать их сохранность и рациональное использование.

5.1.3. Вносить и выносить средства вычислительной техники на территорию Общества только в соответствии с установленными правилами пропускного и внутриобъектового режимов.

5.1.4. Своевременно обновлять личные данные в разделе «Мои контакты» для получения и восстановления пароля.

5.1.5. Сменить первоначальный пароль при первом входе в корпоративную информационную систему.

5.1.6. Обеспечить хранение паролей в электронном виде с использованием специализированного программного обеспечения, принятого к использованию в ГК «Северсталь». Пароли на бумажном носителе хранить в запечатанном конверте в металлическом шкафу или сейфе.

5.1.7. В течение 14 календарных дней с момента создания учётной записи пройти обязательный первичный инструктаж по информационной безопасности. Инструктаж проводится дистанционно через корпоративную систему обучения либо очно с работником УИБ.

5.2. Обязанности при использовании информационных ресурсов

5.2.1. Оформлять запросы через Каталог ИТ-услуг для получения дополнительных прав доступа, установки программного обеспечения и решения технических проблем.

5.2.2. Обратиться к **Инструкции по самостоятельному обновлению баз антивируса** в случаях появления в области уведомлений операционной системы сообщений типа «установка обновления – сбой» или других подобных ошибок обновления баз антивирусной защиты.

5.2.3. Следовать рекомендациям персонала корпоративного ИТ-подразделения по вопросам работоспособности ИТ-сервисов и СВТ.

5.2.4. Безотлагательно исполнять требования работников УИБ, касающиеся вопросов информационной безопасности, а также предоставлять необходимые пояснения по их запросам.

5.2.5. Своевременно обрабатывать уведомления от средств мониторинга и контроля информационной безопасности, выполнять требуемые действия в установленные сроки.

5.2.6. Предоставлять доступ к СВТ на своем рабочем месте работникам УИБ и корпоративного ИТ-подразделения:

- в экстренных случаях – немедленно;
- в остальных случаях – по предварительному согласованию.

5.2.7. Немедленно информировать корпоративное ИТ-подразделение о следующих инцидентах:

- неполадках в работе КИС, сбоях или поломках оборудования (PC, СВТ);
- некорректной работе средств защиты, подозрительных устройствах или проводах;
- утере/краже оборудования (ПК, мобильные устройства, носители информации);
- самопроизвольных действиях ПО (открытие/закрытие программ, движение курсора).

5.2.8. Немедленно сообщать в УИБ (ib@severstal.com) о:

- фактах или подозрениях несанкционированного доступа к защищаемой информации;
- выявлении подозрительных электронных писем (фишинговые письма);
- компрометации паролей или ключей;
- уязвимостях, ошибках в ПО или настройках защиты;
- подключении неизвестных устройств или лиц к КИС;
- нарушениях требований настоящей Инструкции.

5.2.9. Своевременно, не дожидаясь принудительной установки, обновлять операционную систему и установленное программное обеспечение, следуя уведомлениям Центра программного обеспечения АО «Северсталь-инфоком».

5.2.10. Сохранять документы, необходимые для выполнения должностных обязанностей, на корпоративных сервисах для хранения файлов с целью обеспечения их сохранности и возможности восстановления.

5.2.11. Своевременно переносить данные на зарегистрированные съемные носители информации или файловые ресурсы.

5.2.12. Забирать распечатки с сетевых принтеров сразу после окончания печати.

5.2.13. Направить аргументированную заявку в корпоративное ИТ-подразделение на выделение корпоративных ресурсов, предназначенных для обмена файлами большого объема или общего использования файлов несколькими пользователями.

5.3. Обязанности при удалённой работе

5.3.1. Соблюдать требования для работников Общества по информационной безопасности, выезжая за пределы страны в отпуск или командировку.

5.3.2. Не предоставлять третьим лицам, включая членов семьи и друзей, доступ к рабочей информации во время удаленной работы с ресурсами КИС.

5.3.3. Не оставлять без наблюдения в небезопасных условиях рабочую станцию и прочее оборудование, предназначенное для удаленного доступа к ресурсам КИС.

5.3.4. Завершать активные сеансы удаленного доступа сразу после окончания работы с ресурсами КИС и избегать использования общедоступных сетей.

5.3.5. Подключать рабочую станцию к защищенному корпоративному каналу (VPN-Corp) не реже одного раза в месяц для обновления программного обеспечения.

5.4. **Обязанности при изменении должностных функций**

5.4.1. Сдать ответственному лицу либо ответственному работнику корпоративного ИТ-подразделения предоставленные средства вычислительной техники (СВТ) в случае изменения должностных обязанностей, которые не будут связаны с использованием СВТ.

5.4.2. Оформить необходимые запросы в Каталоге ИТ-услуг для отключения неактуальных прав доступа к информационным ресурсам при изменении должностных обязанностей.

5.5. **Обязанности при прекращение трудовых обязательств**

5.5.1. Сдать ответственному лицу либо ответственному работнику корпоративного ИТ-подразделения предоставленные СВТ.

5.5.2. Передать непосредственному руководителю либо ответственному работнику корпоративного ИТ-подразделения материальные носители со служебной информацией, ключи доступа и лицензии на ПО. Материальные носители с защищаемой информацией передаются только непосредственному руководителю или иному уполномоченному лицу в соответствии с локальным нормативным актом.

6. ЗАПРЕЩЁННЫЕ ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЯ

6.1. **При подключении и использовании оборудования**

6.1.1. Оставлять рабочую станцию без активации функции блокировки, за исключением производственной необходимости функционирования без блокировки, разрешенной внутренними регламентами предприятия.

6.1.2. Самовольно подключать и отключать оборудование от КИС без согласования с работниками корпоративного ИТ-подразделения.

6.1.3. Подключать личное оборудование к КИС, за исключением корпоративных гостевых сетей и корпоративных каналов удаленного доступа.

6.1.4. Осуществлять обработку и хранение защищаемой информации на незарегистрированных (личных) съемных носителях информации.

6.1.5. Передавать зарегистрированные съемные носители информации третьим лицам за исключением случаев, предусмотренных соглашениями о конфиденциальности.

6.1.6. Использовать зарегистрированные съемные носители информации в нарушение требований локальных нормативных актов Общества.

6.1.7. Несанкционированно подключать к устройствам, входящим в состав КИС, незарегистрированные съёмные носители информации. Согласование возможности

подключения незарегистрированных устройств осуществляется через каталог ИТ-услуг по соответствующей заявке.

6.1.8. Подключать СВТ к корпоративным гостевым сетям.

6.1.9. Несанкционировано подключать личное оборудование к СВТ.

6.1.10. Использовать СВТ и предоставленные пользователю ресурсы в целях, не связанных с исполнением работником своих должностных обязанностей, хранить информацию, не относящуюся к производственной деятельности (фотографии, фильмы, видеоролики и иные файлы).

6.1.11. Разбирать СВТ, нарушать комплектность выданных СВТ (обмениваться мониторами, и другими комплектующими).

6.1.12. Вносить несанкционированные изменения в конфигурацию программно-аппаратных средств рабочих станций (в том числе вскрывать системные блоки), изменять конфигурацию СВТ, менять параметры BIOS, самовольно устанавливать ПО и обновления, ремонтировать или привлекать к ремонту СВТ работников Общества, кроме персонала корпоративного ИТ-подразделения или сторонней организации, оказывающей ИТ-услуги в соответствии с заключенным договором.

6.1.13. Заниматься модификацией, хищением и уничтожением любых компонентов КИС.

6.2. **При использовании каналов связи и организации точек доступа**

6.2.1. Создавать внутри КИС Общества дополнительные несанкционированные каналы обмена информацией с внутренними или внешними абонентами.

6.2.2. Самостоятельно создавать на рабочих станциях общие сетевые ресурсы, включая файловые папки и иные элементы инфраструктуры общего доступа (в т.ч. FTP и WEB сервера), объединять рабочие станции в локальные сети.

6.2.3. Создавать на территории Общества и подключать к КИС несанкционированные беспроводные точки доступа, подключать к ним принадлежащие Обществу СВТ.

6.2.4. Использовать на подключенных к КИС СВТ посторонние каналы доступа в Интернет (в т. ч. мобильные и некорпоративные беспроводные сети передачи данных), находясь на территории Общества.

6.2.5. Использовать некорпоративное программное обеспечение для организации защищенных каналов VPN, сторонние VPN-сервисы, прочие сервисы проксирования трафика и любые другие некорпоративные средства для сокрытия сетевой активности при подключении к КИС, а также при использовании доступных из сети Интернет корпоративных ресурсов.

6.2.6. Несанкционированно использовать любые средства для организации удаленного доступа и управления рабочими станциями в КИС.

6.2.7. Использовать любые средства для обхода корпоративных средств защиты.

6.3. **При работе с информационными ресурсами**

6.3.1. Производить несанкционированное копирование и хранение информации на ресурсах, не принадлежащих ГК Северсталь и не используемых в рамках заключенных договоров.

6.3.2. Хранить пароли и иные коды для проверки подлинности учетной записи пользователя в открытом виде.

6.3.3. Регистрироваться и работать в КИС под чужим логином и паролем (идентификатором доступа) или кому-либо передавать их.

6.3.4. Предоставлять третьим лицам несанкционированный доступ к рабочей станции и ИТ-ресурсам Общества, регистрационным данным в информационных системах (логины, пароли, секретные ключи), секретным кодам и сведениям, раскрывающим организацию структурных элементов информационных систем.

6.3.5. Использовать стандартные возможности операционных систем или любое другое специальное программное обеспечение для незаконных проверок безопасности, попыток несанкционированного проникновения в КИС и выполнения других подобных действий.

6.3.6. Выключать или деактивировать на рабочих станциях встроенные корпоративные средства администрирования, контроля и защиты.

6.3.7. Использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты, которые могут привести к возникновению компьютерных инцидентов или сбоев в работе КИС.

6.3.8. Самовольно создавать на рабочих станциях локальные виртуальные машины, несколько загрузочных копий операционных систем, несанкционированно производить загрузку рабочей станции с внешних носителей информации.

6.3.9. Устанавливать на рабочую станцию **программное обеспечение, запрещенное к использованию**.

6.3.10. Использовать средства защиты информации, не согласованные УИБ.

6.4. **При работе с конфиденциальной информацией и интернет**

6.4.1. Производить несанкционированное распространение за пределы Общества служебной (рабочей) информации, полученной при работе в КИС.

6.4.2. Осуществлять массовую рассылку электронных сообщений, не относящихся к выполнению функциональных обязанностей.

6.4.3. Осуществлять в рамках функциональных обязанностей массовую рассылку на работников Общества электронных сообщений без подписания их электронной цифровой подписью.

6.4.4. Распространять, отправлять, передавать, воспроизводить, предоставлять или любым иным образом использовать материалы, находящиеся под защитой авторских прав, торговых марок, патентов, режима коммерческой тайны или иных объектов интеллектуальной

собственности, полученные через КСПД, без согласия правообладателя или уполномоченного лица.

6.4.5. Использовать адрес корпоративной электронной почты для регистрации и/или оформления подписок на сайтах, содержание которых не связано с выполнением служебных обязанностей пользователя.

6.4.6. Публиковать без необходимости свой адрес корпоративной электронной почты, либо адреса других работников Общества на общедоступных Интернет-ресурсах (форумы, конференции и т.п.), содержание которых не связано с выполнением служебных обязанностей пользователя.

6.4.7. Использовать некорпоративную электронную почту для ведения служебной переписки, в том числе web-интерфейсы публичных почтовых сервисов yandex.ru, mail.ru, hotmail.com и иных почтовых систем без согласования руководителя подразделения.

6.4.8. Передавать или публиковать в сети Интернет непристойные, клеветнические, оскорбительные, угрожающие или другие противозаконные материалы, распространять материалы, способствующие разжиганию национальной розни, подстрекающие к насилию, призывающие к совершению противоправной деятельности, в том числе разъясняющие порядок применения взрывчатых веществ и иного оружия, распространять вирусы или другие компьютерные коды, файлы или программы, предназначенные для нарушения, уничтожения либо ограничения функциональности любого компьютерного или телекоммуникационного оборудования или программы, для осуществления несанкционированного доступа, а также серийные номера к коммерческим программным продуктам и программы для их генерации, логины, пароли и прочие средства для получения несанкционированного доступа к платным ресурсам в Интернете, а также размещения ссылок на вышеуказанную информацию.

6.4.9. Загружать файлы из сети Интернет (в том числе аудио- и видеофайлы), а также воспроизводить аудио- и видеопотоки (сервисы онлайн-аудио, радио, онлайн-видео, телевидение), не относящиеся к служебной деятельности.

6.4.10. Запускать исполняемые файлы, загруженные из Интернет или с внешних съемных носителей информации, без проверки средствами антивирусной защиты.

6.4.11. Размещать в публичных мессенджерах выраженную в любой форме информацию, сбор и распространение которой ограничен внутренними нормативными документами

6.4.12. Использовать социальные сети и форумы для ведения служебной переписки в нарушение «Положения по использованию публичных и корпоративных социальных медиа и мессенджеров».

6.4.13. Нажимать на рекламные окна, отвечать утвердительно на всплывающие баннеры и предложения веб-браузера «о проверке компьютера на наличие вирусов, уязвимостей, установки программного обеспечения и т. п».

6.4.14. Использовать предоставленный доступ в Интернет в целях рекламирования

товаров и услуг, не связанных с деятельностью Общества.

6.4.15. Нарушать правила операторов связи и владельцев интернет-ресурсов, причинять вред другим пользователям сети и оператору связи.

6.4.16. Использовать сервисы для сокрытия, преобразования, сокращения ссылок для доступа к внешним и внутренним веб-ресурсам (сайтам, страницам) и документам.

7. ПОЛНОМОЧИЯ И ОТВЕТСТВЕННОСТЬ ДОЛЖНОСТНЫХ ЛИЦ

7.1. В случаях нарушения требований настоящей Инструкции пользователи несут уголовную, административную, дисциплинарную и гражданско-правовую ответственность в порядке, установленном законодательством.

7.2. В целях обеспечения устойчивой и безопасной работы информационных систем Общества работники УИБ и персонал корпоративного ИТ-подразделения имеют право осуществлять периодический контроль за работой пользователей и выполнением ими предписаний настоящей Инструкции. Инциденты, связанные с нарушением установленных правил работы, подлежат служебному расследованию.

7.3. В случае нарушения пользователем требований данной Инструкции, которое привело или может привести к возникновению угроз Обществу, работники УИБ и персонал корпоративного ИТ-подразделения имеют право отключить рабочую станцию пользователя от всех сервисов корпоративной сети Общества и (или) заблокировать его учетную запись до устранения негативных факторов.

7.4. Работодатель имеет право прекратить/ограничить доступ к отдельным информационным ресурсам и критичным полномочиям в случае поступления заявления на увольнение от работника Общества.

8. КОНТРОЛЬ ЗА ИСПОЛНЕНИЕМ ИНСТРУКЦИИ

8.1. Контроль за исполнением настоящей Инструкции в структурных подразделениях Обществ возлагается на руководителей данных структурных подразделений.

8.2. Общий контроль за исполнением настоящей Инструкции возлагается на подразделение обеспечения бизнеса в Обществах.

8.3. Данная Инструкция доводится под подпись до всех пользователей, зарегистрированных в КИС.

9. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ В ИНСТРУКЦИЮ

9.1. Период пересмотра настоящей Инструкции – не реже одного раза в 5 лет.

9.2. Общую ответственность за актуальность Инструкции несёт УИБ.

9.3. Согласно требованиям системы менеджмента качества, используются стандартные процедуры работы с документом:

- работа по внесению изменений в документ может быть инициирована любым должностным лицом Общества, заинтересованным в улучшении организации работ;
- изменения в документ в течение срока его действия вносятся с согласования с должностным лицом, несущим общую ответственность за актуальность документа;
- продление срока действия инструкции проводится по окончании срока ее действия на основании положительного решения должностного лица, ответственного за актуальность документа;
- пересмотр инструкции по окончании срока его действия проводится аналогично процедуре внесения изменений в течение срока действия инструкции;
- документ подлежит обязательной актуализации при изменении управленческих документов, связанных с данной бизнес-процедурой.