Публичное акционерное общество
НОВОЛИПЕЦКИЙ МЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ

УТВЕРЖДАЮ

Вице-президент по цифровой трансформации и информационным технологиям

(утверждено) Д.А. Холкин

« 04 » февраля 2021 г.

ПОЛОЖЕНИЕ
об обеспечении информационной безопасности

П DIT-345-0024-2020

(Взамен П IT-162-0024-2019 Положение о допустимом использовании и защите активов, утвержденного 27.11.2019)

Введено в действие распоряжением от « 05 » февраля 2021 года № 1-124-Р-ОД

Дата введения « 05 » февраля 2021 года

Содержание

1. ОБЛАСТЬ ПРИМЕНЕНИЯ

1.1. Настоящее Положение об обеспечении информационной безопасности (далее – положение) устанавливает обязанности работников по соблюдению требований информационной безопасности.

1.2. Настоящее положение разработано в развитие Регламента по информационной безопасности предприятий [1] (**приложение Б**).

1.3. Требования настоящего положения распространяются на деятельность всех структурных подразделений компании и подрядные (субподрядные) организации.

1.4. Требования настоящего положения являются обязательными для соблюдения всеми работниками компании, подрядчиками (субподрядчиками), использующими для выполнения должностных обязанностей информационные системы и автоматизированные системы управления технологическими процессами. Данные сотрудники должны быть ознакомлены с требованиями настоящего положения.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

2.1. В настоящем положении применены термины с соответствующими определениями (см. **приложение А**) в соответствии с Единым корпоративным глоссарием «Термины и определения», размещенном на корпоративном портале в разделе **«**Сервисы\Общие сервисы\Нормативные документы**»: информация; информация, составляющая коммерческую тайну; конфиденциальность информации; работник; руководитель.**

2.2. Дополнительно в настоящем положении применены термины с соответствующими определениями (см. **приложение А**): **автоматизированная система управления технологическими процессами; должностные обязанности; защита информации; информация ограниченного доступа.**

3. СОКРАЩЕНИЯ

3.1. В настоящем положении применены следующие сокращения:

3.1.1. **АСУ ТП:** Автоматизированная система управления технологическим процессом.

3.1.2. **ИС:** Информационная система.

3.1.3. **ПК:** Персональный компьютер.

4. РОЛИ

4.1. Перечень ролей, используемых в настоящем положении, с определениями приведен в таблице 1.

Таблица 1 – Перечень ролей

Роль	Определение
Служба информационной безопасности	Подразделение компании, на которое возложены функции по обеспечению информационной безопасности в компании; подразделение, осуществляющее общее руководство информационной безопасностью в компании
Служба поддержки пользователей	Подразделение компании, осуществляющее техническую поддержку пользователей при работе с информационными системами компании

5. ОСНОВНЫЕ ПОЛОЖЕНИЯ

5.1. К сведениям, составляющим коммерческую тайну, относятся сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны. Порядок обработки сведений, составляющих коммерческую тайну, определен в Положении об управлении информацией, содержащей коммерческую тайну [2].

5.2. Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). Порядок обработки персональных данных определен в Положении об обработке и защите персональных данных [3].

5.3. К информации ограниченного доступа относятся сведения о сферах деятельности компании, доступ к которым ограничивается служебной необходимостью, и разглашение или утрата которых может нанести ущерб компании; сведения ограниченного доступа, которые могут быть использованы для нанесения ущерба компании, в частности к таким сведениям относятся сведения о конфигурации и топологии вычислительной сети, аутентификационная информация, сведения о системе защиты активов компании.

5.4. При работе с защищаемой в компании информацией (персональные данные, сведения, составляющие коммерческую тайну, информация ограниченного доступа) работникам запрещается:

- разглашать защищаемую информацию;
- использовать защищаемую информацию в личных целях;
- оставлять носители с защищаемой информацией (в том числе бумажные) без присмотра;
- передавать носители с защищаемой информацией (в том числе бумажные) посторонним лицам или другим работникам, не имеющим доступ к этой информации;
- передавать защищаемую информацию в общедоступные или непредназначенные для обработки защищаемой информации системы (сервисы обмена файлами Google Docs, Yandex Disk, Облако@mail.ru и аналогичные, незащищенные почтовые системы и иные ресурсы сети Интернет).

5.5. Работники обязаны:

- соблюдать конфиденциальность информации; не разглашать сведения, подлежащие защите (персональные данные, сведения, составляющие коммерческую тайну, информация ограниченного доступа);
- использовать предоставленный доступ к ИС/АСУ ТП компании только в целях выполнения должностных обязанностей;
- при работе с ИС/АСУ ТП компании руководствоваться инструкциями пользователя к этим системам (при их наличии);

- соблюдать политику «чистого стола»: документы и электронные носители информации, когда они не используются, должны убираться в стол, шкаф или другие предназначенные для этого места;
- при прекращении трудового договора передать работодателю все носители информации, имеющиеся в пользовании работника и содержащие защищаемую в компании информацию;
- сообщать в Службу информационной безопасности обо всех фактах нарушения установленного порядка обращения с защищаемой в компании информацией;
- оказывать содействие в расследовании инцидентов информационной безопасности, в том числе предоставлять объяснения по выявленным фактам нарушений в срок, не превышающий три рабочих дня с момента запроса такого объяснения, если внутренними документами компании не установлен иной срок.

5.6. Средства вычислительной техники и ресурсы ИС/АСУ ТП компании предоставляются работникам только для выполнения должностных обязанностей. Использование вычислительной техники и ресурсов ИС/АСУ ТП в личных целях запрещено.

5.7. Любая информация, созданная, собранная, пересылаемая, обработанная и хранимая работником с использованием ресурсов компании, является собственностью компании и может подвергаться контролю.

5.8. При выявлении инцидентов информационной безопасности, появлении признаков некорректного функционирования средств защиты информации работникам следует немедленно сообщить в Службу информационной безопасности. Работникам запрещено предпринимать попытки пресечь инцидент самостоятельно, а также рассказывать об инциденте посторонним лицам.

Также в Службу информационной безопасности необходимо сообщать о возникновении подозрений нарушения информационной безопасности, в том числе о случаях:

- обращения незнакомых лиц с просьбами о предоставлении защищаемой в компании информации;
- выявления фактов несанкционированного распространения, предоставления защищаемой в компании информации, нарушения правил хранения защищаемой в компании информации;
- выявления фактов нарушения правил информационной безопасности;
- утери или кражи оборудования (персонального компьютера, ноутбука и иных мобильных устройств, съемных носителей информации).

Контакты Службы информационной безопасности: nl-soc-operator@nlmk.com

6. ПРАВИЛА ОБРАЩЕНИЯ С ТЕХНИЧЕСКИМИ СРЕДСТВАМИ И ИНФОРМАЦИОННЫМИ РЕСУРСАМИ

6.1. Правила работы с персональным компьютером

6.1.1. Работа с информационными ресурсами и системами разрешена с использованием закрепленного за работником ПК. При наличии производственной необходимости допускается применение одного ПК для работы нескольких работников при условии, что работа каждого осуществляется под персонифицированной учетной записью.

При работе с АСУ ТП использование одного и того же имени пользователя несколькими сотрудниками («группового имени») разрешено только при наличии производственной необходимости (например, при невозможности реализации технологического процесса без применения групповых имен).

6.1.2. Работникам запрещено:

- подключаться к сетям компании с личных устройств, за исключением подключения с использованием личных мобильных устройств к системе корпоративной электронной почты и Skype for Business, удаленной работы с ресурсами компании, организованной посредством Cisco VPN или RDP-клиента, подключения к гостевым беспроводным сетям компании;
- использовать ПК для развлечений и других действий, не связанных с производственными целями компании;
- вскрывать системные блоки и иные компоненты ПК и самостоятельно производить ремонт ПК;
- использовать для работы с системами и сервисами компании устройства третьих лиц;
- подключать к ПК модемы, мобильные телефоны с целью организации точек доступа (в режиме «модем») и другое оборудование, не связанное непосредственно с должностными обязанностями работника;
- самостоятельно устанавливать программное обеспечение, за исключением случаев, когда работник обладает правами локального администратора в соответствии с Положением о процессе управления доступом [4];
- вносить изменения в настройки операционной системы и прикладного программного обеспечения, установленного на ПК;
- вносить изменения в базовую конфигурацию АСУ ТП и ее средства (механизмы) защиты, если такие действия не входят в должностные обязанности работника;
- отключать и/или удалять установленные средства защиты информации, а также изменять их настройки;
- препятствовать работе средств защите информации и автоматизированных средств мониторинга и контроля информационных ресурсов;
- использовать системы виртуализации на рабочих станциях;
- пытаться обойти существующие ограничения своего уровня доступа к ресурсам ИС/АСУ ТП компании;
- осуществлять работу под учетной записью, имеющей права администратора, кроме случаев, установленных в Положении о процессе управления доступом [4]; добавлять учетные записи в привилегированные доменные группы и привилегированные локальные группы пользователей без согласования Службы информационной безопасности;
- осуществлять работу в корпоративной сети под чужой учетной записью;
- предоставлять доступ работникам компании (за исключением администраторов ИС и сотрудников Службы информационной безопасности) и третьим лицам к своему ПК (за исключением лиц, обслуживающих ПК, в том числе по договору с компанией);

- организовывать на ПК ресурсы общего доступа и сетевые сервисы (открывать доступ к общим папкам, дискам, настраивать службы удаленного доступа, беспроводные точки доступа и т.д.);
- осуществлять сканирование сетевых узлов по конечным устройствам или портам, если такая деятельность не связана с выполнением должностных обязанностей;
- хранить и использовать на ПК программное обеспечение, аудио- и видеофайлы, фотографии, не относящиеся к производственной деятельности, объекты интеллектуальной собственности в нарушение прав их законных правообладателей.

6.1.3. При покидании рабочего места работники должны заблокировать компьютер (в операционной системе Windows путем нажатия сочетания клавиш Win+L или сочетания клавиш Ctrl+Alt+Del, а затем кнопки «Блокировка») или выключить компьютер.

6.1.4. В случае если при работах по изменению аппаратно-программной конфигурации закрепленного за ним ПК требуется использование учетной записи работника, работник должен присутствовать при таких работах.

6.2. **Правила работы с мобильными устройствами**

6.2.1. Мобильные устройства в компании используются только в производственных целях для выполнения должностных обязанностей, связанных с необходимостью удаленной работы (например, командировки, работа из дома) с ресурсами компании.

6.2.2. К мобильным устройствам, разрешенным для использования в компании, относятся переносные ПК (ноутбуки, нетбуки), планшеты и мобильные телефоны. Ноутбуки и нетбуки, находящиеся в собственности компании, должны быть введены в домен. Ноутбуки и нетбуки, используемые при работе с АСУ ТП, могут не вводиться в домен при наличии производственной необходимости.

6.2.3. При использовании мобильных устройств работниками должны выполняться все правила работы с персональным компьютером, приведенные в подразделе 6.1 настоящего положения.

6.2.4. Работники несут ответственность за физическую безопасность выданных им мобильных устройств. Если устройство было украдено или утеряно, работнику необходимо незамедлительно сообщить об этом в Службу информационной безопасности.

6.2.5. Работникам запрещено:

- позволять членам своих семей или посторонним лицам использовать мобильные устройства компании;
- использовать мобильные устройства компании для развлечений и других действий, не связанных с выполнением должностных обязанностей;
- бесконтрольно оставлять мобильные устройства компании при транспортировке и хранении;
- сдавать мобильные устройства компании в аэропорту в качестве багажа;
- отключать средства защиты информации на используемых мобильных устройствах компании.

6.3. Правила работы с копировально-множительной техникой

6.3.1. Сервисы сетевой печати и копировально-множительная техника должны использоваться работниками исключительно в служебных целях.

6.3.2. При использовании сервисов сетевой печати и копировально-множительной техники работник обязан:

- сразу забирать из принтеров напечатанные документы;
- хранить созданные им бумажные документы в защищенных от посторонних лиц местах (столы, сейфы, запираемые на ключ шкафы, специализированные помещения);
- уничтожать бумажные носители, содержащие защищаемую в компании информацию, при отсутствии необходимости дальнейшего использования или утрате практической и исторической ценности информации.

6.3.3. Работникам запрещено использование копировально-множительной техники для печати или копирования материалов, не связанных с производственными целями компании и (или) способного нанести ущерб компании.

6.4. Правила парольной защиты

6.4.1. Для идентификации работника и защиты информации от неавторизованного использования или просмотра, при трудоустройстве ему выдается имя пользователя (имя учетной записи) и пароль.

Для выполнения работ, требующих привилегированных полномочий, пользователю по запросу создаются специализированные (административные) учетные записи.

6.4.2. При первом входе в систему работник обязан сменить пароль. Выбор и смену пароля работник должен осуществлять самостоятельно без привлечения других лиц. Смена пароля осуществляется пользователем самостоятельно для персональной учетной записи и для всех учетных записей специального назначения, закрепленных за пользователем.

6.4.3. Требования к паролям пользователей:

- длина пароля должна быть не менее 9 символов;
- в составе символов пароля должны присутствовать буквы латинского алфавита в верхнем и нижнем регистрах, цифры и, при наличии технической возможности, специальные символы (например, ~ ! @ # $ % ^ & * ( ) - + _ = \ | / ? ,);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, обозначение месяца или времени года, указание текущего года), последовательности символов и знаков (например, 111, qwerty, abcd), общепринятые сокращения (например, LAN, HTTP, USER), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетаний букв и знаков, которые можно угадать, основываясь на знании информации о работнике;
- смена пароля должна осуществляться не реже чем 1 раз в 100 календарных дней;
- при смене пароля новое значение должно отличаться от предыдущего не менее, чем в трех позициях.

6.4.4. Работникам запрещена передача паролей третьим лицам (в том числе сотрудникам Службы поддержки пользователей, администратору, непосредственному руководителю и коллегам). При подозрении, что пароль стал известен третьим лицам, работник должен немедленно произвести смену пароля, либо обратиться в единую Службу поддержки пользователей для получения помощи в смене пароля. Служба информационной безопасности оставляет за собой право инициировать внеочередную смену пароля при подозрении на его компрометацию.

6.4.5. Работники обязаны принимать меры по предотвращению ознакомления с паролем посторонних лиц. Запрещается передавать атрибуты своих учетных записей другим лицам, а также хранить их в местах, легко доступных посторонним лицам, хранить пароли в файлах в открытом виде на рабочем месте, хранить аутентификационную информацию в скриптах.

7. ПРАВИЛА ПЕРЕДАЧИ ИНФОРМАЦИИ

7.1. Правила работы с электронной почтой и сервисами мгновенных сообщений

7.1.1. Прием и отправка сообщений электронной почты осуществляется работниками с использованием корпоративной почтовой системы. Использование сторонних почтовых сервисов и сторонних почтовых клиентов запрещено.

7.1.2. Прием и отправка мгновенных сообщений, организация видеоконференций осуществляется работниками с использованием корпоративной системы Skype for business, ПО Zoom. Использование иных сервисов мгновенных сообщений разрешено только по согласованию со Службой информационной безопасности.

7.1.3. Если почтовое сообщение содержит информацию, подлежащую защите в компании (персональные данные, сведения, составляющие коммерческую тайну, информация ограниченного доступа), подпись работника – отправителя сообщения должна содержать строки следующего содержания:

«Настоящее письмо и приложения к нему содержат информацию, подлежащую защите в «Наименование компании», и охраняются законодательством.

Указанная информация не может быть использована, скопирована или разглашена Вами, если согласие на выполнение таких действий ранее не было предоставлено Вам обладателем такой информации.

Если Вы получили это письмо по ошибке, незамедлительно сообщите об этом отправителю письма и удалите письмо и приложения к нему».

«This letter and its attachments contain information that is subject to protection in the "Company Name" and are protected by law.

The specified information cannot be used, copied or disclosed if the consent to perform such actions was not previously provided to you by the owner of such information.

If you received this letter by mistake, immediately inform the sender and delete the letter and its attachments».

7.1.4. Работникам запрещено:

- отвечать на сообщения, переходить по ссылкам и открывать файлы вложения, если отправитель не известен, либо сообщение сомнительного содержания;

- пересылать подозрительные сообщения работникам компании (за исключением пересылки таких сообщений в Службу поддержки пользователей для анализа);
- использовать сервисы электронной почты и мгновенных сообщений для отправки сообщений, нарушающих требования действующего законодательства, нормы корпоративной этики и культуры, сообщений оскорбительного, непристойного содержания, агитации, пропаганды религиозных или политических идей, нежелательных почтовых сообщений (спама), сообщений рекламного характера и других целей, которые влекут нанесение компании материального ущерба или ущерба ее деловой репутации;
- осуществлять массовую рассылку почтовых сообщений (более 50 адресатов), если это не предусмотрено должностными обязанностями работника;
- осуществлять частную переписку с использованием сервисов компании. К частной переписке относится переписка, не связанная с исполнением работником своих должностных обязанностей;
- настраивать автоматическую переадресацию получаемых сообщений на почтовые адреса, открытые на сторонних почтовых сервисах (автоматическую пересылку всех сообщений, отправленных пользователю, на другой почтовый адрес на стороннем почтовом сервисе);
- отправлять сообщения с использованием поддельных учетных записей;
- читать, отправлять, удалять чужие (не адресованные работнику) сообщения, если соответствующие права не были делегированы ему работодателем. Письма, содержащие вредоносные вложения и ссылки, могут быть удалены автоматически.

7.1.5. Передача документов, содержащих персональные данные, по электронной почте осуществляется в архиве с паролем, при этом пароль от архива передается адресату с помощью альтернативного канала связи (например, в виде SMS-сообщения или посредством Skype for Business). Передача документов, содержащих персональные данные, по электронной почте допускается без применения требования по отправке файлов в архиве с паролем в следующих случаях:

- внутри компании или в общекорпоративной переписке;
- в государственные/правоохранительные органы, саморегулируемые организации (СРО), нотариальные конторы в связи с выполнением государственных и/или нотариальных функций по отношению к деятельности компании (исключая бесплатные почтовые сервисы, например, @yandex.ru, @mail.ru, @rambler.ru);
- партнерам/контрагентам исключительно в целях выполнения должностных обязанностей и только на официальные почтовые ящики партнеров/контрагентов (исключая бесплатные почтовые сервисы, например, @yandex.ru, @mail.ru, @rambler.ru).

7.1.5.1. В исключительных случаях, при служебной необходимости отправки документов, содержащих персональные данные, на бесплатные почтовые сервисы, например, @yandex.ru, @mail.ru, @rambler.ru, необходимо:

- согласовать по корпоративной электронной почте необходимость данной отправки с непосредственным руководителем либо со Службой

информационной безопасности, выбрав в адресной книге электронный почтовый ящик – «*Согласование передачи информации УИБ*»;

- заархивировать и отправить документы получателю. Требования по архивации не применимы к отправке файлов в государственные/правоохранительные органы, саморегулируемые организации (СРО), нотариальные конторы;
- выслать архив и пароль от архива на корпоративный почтовый ящик Службы информационной безопасности, выбрав в адресной книге электронный почтовый ящик – «*Согласование передачи информации УИБ*».

7.1.6. Работники обязаны:

- быть особенно внимательными при открытии вложений в сообщениях корпоративной электронной почты или корпоративных сервисов «мгновенных» сообщений, полученных от неизвестных отправителей, так как они могут содержать вредоносное ПО;
- обращать внимание на адрес отправителя, оформление письма, правильность ссылки в адресной строке при переходе по ссылкам, полученным в письме: часто злоумышленники используют похожие по написанию доменные имена (например, g00gle.com вместо google.com). В случае подозрений на мошенничество, не открывать вложения и не переходить по ссылкам, содержащимся в письме;
- с целью недопущения разглашения защищаемой информации, перед отправкой сообщения или письма еще раз проверить, тому ли адресату оно отправляется, а также исключить из получателей тех, кому оно не предназначено.

7.2. Правила работы с файловыми хранилищами

7.2.1. Для обмена информацией в электронном виде с сотрудниками сторонних организаций по ссылкам или организации общего доступа к файлам, а также для целей резервного копирования информации используется корпоративное хранилище NLMK-cloud (https://drive.nlmk.com/) и корпоративное хранилище SharePoint. Корпоративное хранилище NLMK-cloud используется для выполнения должностных обязанностей, использование хранилища в иных целях запрещено.

7.2.2. Прием и передача информации, размещенной на корпоративном хранилище NLMK-cloud, по ссылкам сотрудникам сторонних организаций или организация общего доступа к файлам разрешены сотрудникам уровня «начальник управления» и выше для выполнения должностных обязанностей. При необходимости осуществления приема и передачи информации, размещенной на корпоративном хранилище NLMK-cloud, по ссылкам сотрудникам сторонних организаций или организации общего доступа к файлам сотрудникам ниже уровня «начальник управления», необходимо:

- согласовать по корпоративной электронной почте предоставление такого доступа с руководителем структурного подразделения;
- создать заявку на формирование ссылок в Службу поддержки пользователей, указав обоснование необходимости такого доступа, и приложить полученное согласование руководителя структурного подразделения. После исполнения

заявки будет предоставлен доступ на формирование ссылок для приема и передачи информации, размещенной на корпоративном хранилище NLMK-cloud.

В исключительных случаях, при необходимости хранения и передачи документов, содержащих персональные данные и информацию, составляющую коммерческую тайну, с использованием корпоративного хранилища NLMK-cloud необходимо:

- хранить и передавать защищаемую информацию только в архиве с паролем;
- перед передачей информации третьим лицам выслать архив (или ссылку на архив) и пароль от архива на корпоративный почтовый ящик Службы информационной безопасности, выбрав в адресной книге электронный почтовый ящик – «*Согласование передачи информации УИБ*».

7.2.3. Работникам запрещено:

- хранить защищаемую информацию на ресурсах, для этого не предназначенных;
- использовать для хранения и передачи защищаемой информации внешние файловые ресурсы (например, Google Drive, Microsoft OneDrive, Dropbox, Яндекс.Диск, Облако@mail.ru);
- хранить на корпоративном хранилище NLMK-cloud информацию, не связанную с производственными целями компании и (или) способного нанести ущерб компании;
- хранить на корпоративном хранилище NLMK-cloud информацию, нарушающую авторские права ее владельцев.

7.3. Правила работы со съемными носителями информации

7.3.1. Использование съемных носителей информации на чтение разрешено всем работникам для выполнения должностных обязанностей. Использование съемных носителей информации в иных целях запрещено.

7.3.2. Использование съемных носителей информации на запись для выполнения должностных обязанностей разрешено сотрудникам уровня «начальник управления» и выше. При необходимости использования съемных носителей информации на запись для выполнения должностных обязанностей иным работникам, необходимо:

- согласовать по корпоративной электронной почте предоставление такого доступа с руководителем структурного подразделения;
- создать заявку на использование съемных носителей информации на запись в Службу поддержки пользователей, указав обоснование необходимости такого доступа, и приложить полученное согласование руководителя структурного подразделения. После исполнения заявки будет предоставлен доступ на запись информации на съемные носители информации.

7.3.3. Хранение и передача сведений, составляющих коммерческую тайну, на съемных носителях информации осуществляется в соответствии с требованиями Положения об управлении информацией, содержащей коммерческую тайну [2].

7.3.4. Работники обязаны:

- осуществлять антивирусный контроль съемных носителей информации при их подключении к ПК;

- контролировать перемещение и содержание информации на съемных носителях, исключать доступ третьих лиц к информации, подлежащей защите (персональные данные, сведения, составляющие коммерческую тайну, информация ограниченного доступа);
- обеспечивать физическую безопасность съемных носителей информации всеми разумными способами.

7.3.5. Работникам запрещено:

- передавать съемные носители лицам, не имеющим права на доступ к информации, хранимой на этих носителях;
- хранить информацию на съемных носителях дольше срока, необходимого для выполнения производственных задач;
- использовать съемные носители информации без проведения предварительной антивирусной проверки.

7.4. Правила работы в сети Интернет

7.4.1. Взаимодействие работников с сетью Интернет осуществляется только для выполнения должностных обязанностей.

7.4.2. Работникам предоставляется доступ к базовым сервисам сети Интернет, которые в том числе не включают в себя доступ к социальным сетям, внешним почтовым ресурсам. При необходимости расширения доступа в сеть Интернет, необходимо:

- заполнить заявку на расширение пользовательского доступа в сеть Интернет, указав в обосновании какие технологические действия требуют расширенного доступа. Форма заявки находится на корпоративном портале по адресу https://nlmk.one/services/it_support/;
- согласовать по корпоративной электронной почте предоставление такого доступа с непосредственным руководителем;
- создать заявку на расширение пользовательского доступа в сеть Интернет в Службу поддержки пользователей и приложить полученное согласование непосредственного руководителя.

7.4.3. Работники обязаны:

- перед открытием загруженных из сети Интернет файлов проверять их на отсутствие вредоносного ПО;
- обращать внимание на точное написание Интернет-адресов и автоматические переходы на другие Интернет-ресурсы. В случае подозрений на мошенничество или вредоносный ресурс, не посещать его.

7.4.4. При работе в сети Интернет с использованием информационных ресурсов компании работникам запрещено:

- передавать по сети Интернет информацию, подлежащую защите (персональные данные, сведения, составляющие коммерческую тайну, информация ограниченного доступа), кроме случаев, предусмотренных договорами между компанией и сторонними организациями;

- распространять в сети Интернет информацию, подлежащую защите, публиковать такую информацию на сайтах, форумах, в блогах, социальных сетях, файлообменных сервисах и других ресурсах сети Интернет;
- использовать или публиковать реквизиты доступа к информационным ресурсам компании (имя пользователя, пароль, адрес электронной почты) при регистрации или работе на общедоступных Интернет-ресурсах;
- посещать Интернет-ресурсы, не имеющие отношения к выполнению должностных обязанностей, не связанные с производственными целями компании и (или) способные нанести ущерб компании, в том числе репутационный ущерб;
- посещать ресурсы трансляции потокового видео и аудио, если такая деятельность не связана с выполнением должностных обязанностей;
- загружать из сети Интернет программное обеспечение, исполняемые файлы, если такая деятельность не связана с выполнением должностных обязанностей, а также музыкальные и видео-файлы;
- осуществлять попытки обхода настроек средств защиты информации, прокси-серверов и фаерволов;
- устанавливать и использовать торрент-клиенты;
- использовать технологии и сервисы с целью сокрытия сетевого трафика, обеспечения анонимности работы в сети Интернет, получения доступа к системам передачи данных и сообщений, получения доступа к запрещенным ресурсам;
- использовать любые виртуальные и анонимные сети (TOR, I2P и другие);
- организовывать дополнительные точки доступа к сети Интернет, в том числе с использованием мобильных устройств.

8. МОНИТОРИНГ И КОНТРОЛЬ

8.1. В целях защиты сведений, составляющих коммерческую тайну, и другой защищаемой информации, соблюдения требований нормативных документов в области информационной безопасности и обеспечения необходимого уровня информационной безопасности в целом, в компании применяются автоматизированные средства мониторинга и контроля использования информационных ресурсов.

8.2. Все действия, совершаемые от имени работников в ИС и АСУ ТП компании, могут контролироваться и протоколироваться. Информация о действиях работников в ИС и АСУ ТП компании может быть использована Службой информационной безопасности для расследования инцидентов информационной безопасности.

8.3. Компания оставляет за собой право проводить периодическую проверку персональных компьютеров пользователей, ИС и АСУ ТП с целью обеспечения проверки выполнения требований настоящего положения. Проверка проводится силами Службы информационной безопасности.

8.4. При расследовании инцидентов информационной безопасности Служба информационной безопасности имеет право:

- запрашивать информацию, необходимую для проведения проверок информационной безопасности;
- привлекать к участию в проверках работников структурных подразделений;

- осуществлять доступ к рабочим местам и персональным компьютерам работников;
- отстранять пользователей от работы с компьютерной техникой и ИС в случае возникновения угроз информационной безопасности;
- изымать компьютерную и другую технику, съемные носители, принадлежащие компании, для проведения проверки в случае невозможности ее выполнения на месте.

9. ОТВЕТСТВЕННОСТЬ

9.1. Каждый работник несет личную ответственность за выполнение применимых к нему требований настоящего положения.

9.2. Руководители структурных подразделений несут ответственность за соблюдение требований информационной безопасности в подконтрольных им подразделениях.

9.3. За нарушение требований настоящего положения, законодательства РФ работники могут быть привлечены к дисциплинарной, административной, гражданско-правовой или уголовной ответственности.

9.4. Компания имеет право аннулировать любые привилегии доступа пользователей к информационным системам и сервисам за нарушение предписаний, правил безопасности или за поведение, мешающее нормальной работе компании.

9.5. Ответственность за контроль исполнения требований настоящего положения возложена на начальника Управления информационной безопасности.

ПРИЛОЖЕНИЕ А
(справочное)
ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

А.1. В настоящем положении применены следующие термины с соответствующими определениями в соответствии с Единым корпоративным глоссарием «Термины и определения», размещенном на корпоративном портале в разделе «Сервисы\Общие сервисы\Нормативные документы»:

А.1.1. **Информация**: значимые данные.

А.1.2. **Информация, составляющая коммерческую тайну**: сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

А.1.3. **Конфиденциальность информации**: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

А.1.4. **Работник:** физическое лицо, вступившее в трудовые отношения с предприятием.

А.1.5. **Руководитель:** лицо, осуществляющее руководство дивизионом / функциональным направлением / предприятием / структурным подразделением предприятия.

А.2. Дополнительно в настоящем положении применены следующие термины с соответствующими определениями:

А.2.1. **Автоматизированная система управления технологическими процессами:** комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами.

А.2.2. **Должностные обязанности:** обязанности сотрудника, выполняемые им в рамках занимаемой должности.

А.2.3. **Защита информации:** деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

А.2.4. **Информация ограниченного доступа:** сведения о сферах деятельности компании, доступ к которым ограничивается служебной необходимостью, и разглашение или утрата которых может нанести ущерб компании; сведения ограниченного доступа, которые могут быть использованы для нанесения ущерба компании, в частности к таким сведениям относятся сведения о конфигурации и топологии вычислительной сети, аутентификационная информация, сведения о системе защиты активов компании.

ПРИЛОЖЕНИЕ Б
(справочное)
БИБЛИОГРАФИЯ

[1] Регламент по информационной безопасности предприятий, утвержденный президентом (председателем Правления) 21.05.2015.

[2] П DIT-345-0050-2020 Положение об управлении информацией, содержащей коммерческую тайну, утв. вице-президентом по цифровой трансформации и информационным технологиям 06.08.2020.

[3] П LG-162-0006-2020 Положение об обработке и защите персональных данных, утв. вице-президентом по цифровой трансформации и информационным технологиям 13.01.2021.

[4] П DIT-345-0072-2020 Положение о процессе управления доступом, утв. вице-президентом по цифровой трансформации и информационным технологиям 04.02.2021.