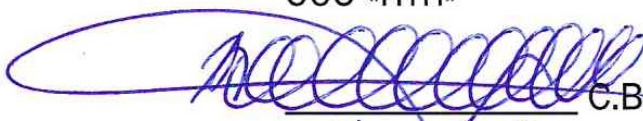


ОБЩЕСТВО С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «ПРИМОРСКИЙ ТОРГОВЫЙ ПОРТ»
(ООО «ПТП»)

УТВЕРЖДАЮ

Генеральный директор
ООО «ПТП»


С.В. Волынец
«14» 07 2020 г.

**ПОЛОЖЕНИЕ
О ПОРЯДКЕ УПРАВЛЕНИЯ ДОСТУПОМ
К ИНФОРМАЦИОННЫМ РЕСУРСАМ ООО «ПТП»**

П-21-ПТП-015-20

г. Приморск
2020 г.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Предисловие

1 ДОКУМЕНТ РАЗРАБОТАН обществом с ограниченной ответственностью «Приморский торговый порт» (ООО «ПТП»)

2 УТВЕРЖДЕН ООО «ПТП»

3 ДАТА ВВЕДЕНИЯ:

4 ВВЕДЕН ВЗАМЕН РД 1900.178-2018 «Регламент предоставления доступа к информационным ресурсам Единой информационной системы ПАО «НМТП» и его дочерних зависимых Обществ

5 СРОК ДЕЙСТВИЯ – до замены (отмены)

6 УКАЗАНИЯ ПО ПРИМЕНЕНИЮ

С даты введения в действие настоящего документа управление доступом к информационным ресурсам следует осуществлять в соответствии с требованиями, установленными настоящим документом

7 Оригинал документа хранится в производственно-техническом отделе ООО «ПТП»

8 Аннотация

Документ устанавливает порядок управления доступом к информационным ресурсам ООО «ПТП»

9 Подразделение ООО «ПТП», ответственное за документ (куратор), – отдел информационных технологий и связи.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Содержание

1	Область применения.....	1
2	Нормативные ссылки.....	1
3	Термины и определения.....	1
4	Обозначения и сокращения.....	4
5	Основные положения.....	5
5.1	Основные положения по управлению доступом.....	5
5.2	Учетные записи.....	5
5.3	Файловые ресурсы.....	7
6	Управление доступом к информационным ресурсам.....	8
6.1	Предоставление доступа.....	8
6.2	Прекращение доступа.....	9
6.3	Пересмотр прав доступа.....	11
7	Управление документами.....	12
7.1	Перечень информационных систем.....	12
7.2	Матрица ролей и полномочий.....	12
	Приложение А (обязательное) Формы заявок.....	14
A.1	Форма заявки на изменение параметров учетной записи.....	14
A.2	Форма заявки на создание или продление срока действия ФР-ресурса.....	15
A.3	Форма заявки на предоставление доступа к ИР.....	17
A.4	Форма заявки на прекращение доступа к ИР.....	19
	Приложение Б (обязательное) Передача учетных данных.....	20
B.1	Общие требования к передаче учетных данных.....	20
B.2	Способы передачи учетных данных.....	20
	Приложение В (рекомендуемое) Форма перечня информационных систем.....	22
	Приложение Г (рекомендуемое) Форма матрицы ролей и полномочий информационной системы.....	23
	Библиография.....	25

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

1 Область применения

1.1 Настоящий документ устанавливает порядок управления доступом к информационным ресурсам ООО «ПТП».

1.2 Настоящий документ предназначен для применения ООО «ПТП», а также организациями, принимающими участие в выполнении работ с использованием информационных ресурсов ООО «ПТП».

2 Нормативные ссылки

В настоящем документе использованы нормативные ссылки на следующие документы:

ОР-03.100.00-КТН-061-19 Положение о защите коммерческой тайны ПАО «Транснефть» и иной конфиденциальной информации

ОР-35.240.00-КТН-001-15 Порядок присвоения имен пользователей, серверов и рабочих станций

ОР-35.240.00-КТН-117-16 Перечень сведений, составляющих коммерческую тайну ПАО «Транснефть» и иных конфиденциальных сведений

ОР-35.240.20-КТН-179-12 Политика парольной защиты в автоматизированных (информационных) системах ОАО АК «Транснефть» и организаций системы «Транснефть»

Примечание – При пользовании настоящим документом целесообразно проверить действие ссылочных документов в соответствии с действующим «Перечнем законодательных актов и основных нормативных и распорядительных документов, действующих в сфере магистрального трубопроводного транспорта нефти и нефтепродуктов». Если ссылочный документ заменен (изменен), то при пользовании настоящим нормативным 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 и определения

В настоящем документе применены следующие термины с соответствующими определениями:

3.1 административная учетная запись: Учетная запись с административными полномочиями, используемая для управления информационной системой.

Примечание – Административные полномочия определяются матрицей ролей и полномочий информационной системы.

3.2 администратор информационной системы: Работник ООО «ПТП», имеющий административные права доступа к информационной системе ООО «ПТП» и отвечающий за ее техническую эксплуатацию и сопровождение.

3.3 администратор учетной записи: Работник ООО «ПТП», наделенный правами администрирования учетных записей.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

3.4 активный каталог (Active Directory): Служба «Активный каталог» в серверных операционных системах.

3.5 базовый пакет информационных ресурсов: Пакет информационных ресурсов, доступ к которым предоставляется при создании основной учетной записи.

Примечания

1. В базовый пакет информационных ресурсов входит: основная учетная запись, личные папки «Мои документы» и «Рабочий стол», электронная почта, общедоступные информационные ресурсы ООО «ПТП».

2. Под общедоступным информационным ресурсом ООО «ПТП» в настоящем документе понимают информационный ресурс, доступ к которому предоставляется для всех учетных записей в домене rtport.ru.

3.6 бизнес-роль: Часть совокупности функций, полномочий и ответственности исполнителя, необходимая для решения определенной задачи его производственной деятельности и закрепленная в должностной инструкции, положении о соответствующем подразделении и иных нормативных документах ООО «ПТП».

3.7 групповая учетная запись: Учетная запись, используемая несколькими работниками, доступ к которой оформлен заявкой на предоставление доступа к информационным ресурсам.

3.8 доступ к информационному ресурсу: Возможность получения информации и ее использования (по Федеральному закону [1]).

3.9 заявитель: Работник, непосредственно участвующий в процессе оформления заявки, осуществляющий организацию процесса согласования и подписания заявки, в том числе комментирование и исправление замечаний, являющийся контактным лицом в процессе выполнения заявки и получающий уведомление о ходе и результатах выполнения.

3.10 заявка: Документ, содержащий намерение работника на доступ к информационным ресурсам, оформленный в установленном порядке.

Примечание – Под заявкой на доступ к информационным ресурсам в настоящем документе понимают заявку на предоставление/прекращение доступа к информационным ресурсам/изменение параметров учетной записи/создание или продление срока действия файлового ресурса.

3.11 информационная система: Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств (по Федеральному закону [1]).

Примечание – Корпоративные информационные системы/инфраструктурные сервисы и службы являются частными случаями информационных систем и предназначены для эксплуатации в рамках корпоративной компьютерной сети ООО «ПТП».

3.12 информационные технологии: Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов (по Федеральному закону [1]).

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

3.13 информационный ресурс: Информация, представленная средствами информационной системы в электронном виде.

3.14 информация: Сведения (сообщения, данные) независимо от формы их представления (по Федеральному закону [1]).

3.15 кадровые уведомления: Уведомления, сформированные сотрудниками отдела управления персоналом ООО «ПТП» на основании приказов.

Примечания

1. Под кадровыми уведомлениями в настоящем документе понимают уведомления, сформированные на основании приказов на заключение трудового договора, прекращение трудового договора, перемещение в другое самостоятельное структурное подразделение внутри одной организации, изменение персональных данных (фамилия/имя/отчество) работника.

3.16 матрица ролей и полномочий информационной системы: Документ в виде таблицы с перечнем ролей информационной системы, соответствующими им правами доступа к информационным ресурсам, разрешающим доступ, а также полем, которое идентифицирует обладателя информации.

3.17 обладатель информации: Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (по Федеральному закону [1]).

3.18 обслуживающий персонал: Специалисты, обеспечивающие разработку, администрирование и поддержку пользователей информационной системы.

3.19 основная учетная запись: Доменная пользовательская учетная запись, не обладающая административными полномочиями, выдаваемая работнику ООО «ПТП» при заключении трудового договора с работником.

3.20 ответственный за размещение информации по доступу: Специалист информационной безопасности, осуществляющий размещение на файловом ресурсе, доступном для чтения всем пользователям корпоративной компьютерной сети ООО «ПТП», актуальной информации по доступу к информационным ресурсам, а также размещение на корпоративном внутреннем портале актуального перечня информационных систем.

3.21 перечень информационных систем: Документ в виде таблицы с перечнем эксплуатируемых и планируемых к внедрению информационных систем с указанием ссылки на матрицу ролей и полномочий информационной системы.

3.22 подтверждающий доступ: Лицо, подтверждающее необходимость доступа к информационным ресурсам путем подписания заявки.

3.23 пользователь: Работник, получивший санкционированный доступ к информационным ресурсам.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

3.24 пользовательская учетная запись: Учетная запись, не обладающая административными полномочиями, предназначенная для работы пользователя с информационными ресурсами.

3.25 разрешающий доступ: Лицо, уполномоченное обладателем информации предоставлять доступ к информационным ресурсам путем согласования заявки.

3.26 система централизованного управления доступом: Корпоративная информационная система, осуществляющая автоматизированный электронный документооборот по согласованию прав доступа пользователей к информационным ресурсам на основе утвержденных ролей и автоматически поддерживающая актуальность данных о пользователях во всех информационных системах, подключенных к ней.

3.27 технологическая учетная запись: Учетная запись, предназначенная для сопровождения информационных систем путем выполнения технологических операций, которые не требуют непосредственного участия администратора или пользователя.

Примечание – Разновидностью технологической учетной записи является групповая управляемая учетная запись, используемая на серверах при запуске служб. Пароль групповой управляемой учетной записи службы меняется автоматически контроллером домена, не перезапуская при этом службы.

3.28 учетная запись: Запись, содержащая сведения для идентификации пользователя при подключении к информационной системе.

Примечания

1. Основные сведения учетной записи (учетные данные) – входное имя (логин) и пароль – используются для доступа в информационную систему, дополнительные сведения – имя, фамилия, отчество, псевдоним (ник), адрес электронной почты, другое – используются для авторизации пользователя.

2. Учетные записи, наделенные соответствующими полномочиями (правами доступа), предоставляют пользователям возможность входить в систему и обращаться к информационным ресурсам.

3.29 файловый ресурс: Информационный ресурс, состоящий из совокупности файлов и папок, опубликованный для общего или ограниченного доступа через файловый сервер.

3.30 функциональный заказчик: Структурное подразделение ООО «ПТП», в интересах которого создана информационная система.

4 Обозначения и сокращения

В настоящем документе применены следующие обозначения и сокращения:

СБ – служба безопасности ООО «ПТП»;

ОИТиС – отдел информационных технологий и связи ООО «ПТП»;

ИС – информационная система;

ИБ – информационная безопасность;

ИС – информационная система;

КИС – корпоративная информационная система;

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

МРиП – матрица ролей и полномочий;
ОСТ – организация системы «Транснефть»;
СУБД – система управления базами данных;
СЦУД – система централизованного управления доступом;
СЭД – система электронного документооборота;
УЗ – учетная запись;
ФР – файловый ресурс;
AD – Active Directory (активный каталог);
FTP – File Transfer Protocol (протокол передачи файлов по сети);
SMB – Server Message Block (сетевой протокол для удаленного доступа).

5 Основные положения

5.1 Основные положения по управлению доступом

5.1.1 Основной целью управления доступом является обеспечение санкционированного доступа пользователей и предотвращение несанкционированного доступа к ИР ООО «ПТП», а также предоставление каждому пользователю таких полномочий доступа к ИР, которые будут являться необходимыми и достаточными для решения возложенных на него задач в соответствии с выполняемыми должностными обязанностями.

5.1.2 Управление доступом к ИР включает процедуры предоставления доступа, прекращения доступа и пересмотра прав доступа.

5.1.3 Доступ к ИР, содержащим сведения, составляющие коммерческую тайну ООО «ПТП», персональные данные, иные конфиденциальные сведения, предоставляется / прекращается в соответствии с ОР-03.100.00-КТН-061-19 и требованиями настоящего документа, к остальным ИР – в соответствии с требованиями настоящего документа.

5.1.4 По вопросам оформления заявок следует обращаться за консультацией в ОИТиС.

5.1.5 Актуальная информация о доступе к ИР (перечень ИС, адрес ФР, на котором размещены МРиП ИС, средства коммуникации для обращения в ОИТиС, другое) размещена на файловом сервере в разделе «Доступ к информационным ресурсам».

5.2 Учетные записи

5.2.1 Доступ к ИР предоставляется пользователям через УЗ.

5.2.2 УЗ подразделяются на следующие категории:

а) по типу:

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

- доменная (создается службой AD домена ООО «ПТП»);
- локальная (создается средствами операционной системы на рабочей станции/сервере/другом оборудовании ООО «ПТП»);

- ИС (создается непосредственно в прикладном программном обеспечении ИС, СУБД);

б) по назначению:

- административная;
- пользовательская;
- технологическая;

в) по принадлежности к организации работника:

- УЗ работника ООО «ПТП»;
- УЗ работника сторонней организации.

5.2.3 Различают следующие виды УЗ, которые могут относиться к любой из категорий, указанных в 5.2.2, в различных комбинациях:

- тестовая;
- групповая.

5.2.4 Для разных категорий УЗ устанавливают различные требования информационной безопасности при оформлении и предоставлении доступа к ИР.

5.2.5 Для доступа к базовому пакету ИР работнику предоставляется доменная пользовательская УЗ, не обладающая административными полномочиями (основная УЗ).

5.2.6 Работа под административными УЗ в ИС допускается только для выполнения административных функций.

5.2.7 Использование групповых УЗ допускается только по решению руководства ООО «ПТП» при отсутствии возможности создания персонифицированных УЗ.

5.2.8 Наименование УЗ – в соответствии с ОР-35.240.00-КТН-001-15.

5.2.9 При создании УЗ администратор УЗ должен установить пароль с опцией (при наличии технической возможности) обязательной смены пароля при первом входе пользователя в ИС. Порядок создания, использования, смены и прекращения действия паролей к УЗ – в соответствии с ОР-35.240.20-КТН-179-12.

5.2.10 Изменение параметров УЗ при изменении фамилии/имени/отчества работника осуществляется на основании:

- кадрового уведомления на изменение персональных данных (фамилия/имя/отчество) работника ООО «ПТП»;

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

- заявки на изменение параметров УЗ, приведенной в А.1(приложение А). Заявка на изменение параметров УЗ должна быть подписана подтверждающим доступ (руководитель подразделения ООО «ПТП»).

5.2.11 Изменение других параметров УЗ пользователя (телефон, месторасположение рабочего места пользователя и т. п.) осуществляют на основании обращения работника в ОИТиС.

5.2.12 Блокировка УЗ пользователя выполняется при превышении количества ввода неверного пароля или обнаружении несанкционированных действий со стороны пользователя по запросу СБ.

5.2.13 Разблокирование или сброс пароля УЗ осуществляется на основании обращения пользователя в ОИТиС в следующих случаях:

- если УЗ была заблокирована в результате превышения количества ввода самим пользователем неверного пароля;
- пользователь забыл пароль;
- истек срок действия начального пароля.

В остальных случаях разблокирование не выполняется до особых указаний СБ.

5.2.14 Способы передачи работнику входного имени (логин) и/или пароля УЗ – в соответствии с приложением Б.

5.3 Файловые ресурсы

5.3.1 Создание или продление срока действия ФР-ресурса должно быть оформлено заявкой в СЭД. Форма заявки на создание или продление срока действия ФР-ресурса приведена в А.2 (приложение А).

5.3.2 При отсутствии приложения к заявке со структурой ресурса и ролями доступа по умолчанию создаются типовые бизнес-роли пользователей с доступом «чтение» и «запись» и соответствующими им группами безопасности в AD домена размещения.

5.3.3 Заявка на создание или продление срока действия ФР-ресурса должна быть согласована с начальником ОИТиС, начальником СБ и подписана руководителем подразделения ООО «ПТП», являющегося инициатором создания ФР-ресурса.

В процессе согласования заявки:

- Начальник ОИТиС – проверяет корректность заполнения полей заявки, анализирует приложение к заявке со структурой ресурса и ролями доступа на предмет технической возможности исполнения;
- начальник СБ – контролирует по направлению деятельности СБ.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

6 Управление доступом к информационным ресурсам

6.1 Предоставление доступа

6.1.1 Основанием для создания основной УЗ является кадровое уведомление о заключении трудового договора с работником.

6.1.2 Процесс предоставления доступа к ИР для работника ООО «ПТП» осуществляется после прохождения им инструктажа в СБ по вопросам обеспечения ИБ, ознакомления данного работника под расписку с установленным в ООО «ПТП» режимом коммерческой тайны и с мерами ответственности за его нарушение, а также после доведения до него требований нормативных документов по парольной и антивирусной защите при передаче учетных данных.

6.1.3 Предоставление доступа к ИР осуществляется на основании заявки, оформленной в СЭД или на бумажном носителе в соответствии с А.3 (приложение А).

6.1.4 Заявку на предоставление доступа к ИР оформляет заявитель, используя актуальный перечень ИС, расположенный на файловом сервере в разделе «Доступ к информационным ресурсам», в порядке, установленном настоящим пунктом.

6.1.4.1 В перечне ИС заявитель находит необходимую ИС.

6.1.4.2 Для выбора необходимой роли ИС заявитель использует актуальную МРиП ИС, ссылка на которую приведена в перечне ИС.

6.1.4.3 При оформлении заявки в СЭД заявитель должен заполнить обязательные поля с последующим направлением заявки на согласование.

6.1.4.4 При оформлении заявки на бумажном носителе заявитель должен заполнить заявку в соответствии с А.3 (приложение А).

Заявка на бумажном носителе оформляется только для сотрудников, у которых нет доступа к СЭД. Согласование заявки осуществляется согласно п. 6.1.4.7.

6.1.4.5 Если в заявке невозможно указать все необходимые для предоставления доступа технические параметры КИС, то допускается использовать дополнительное приложение к заявке, в котором в виде таблицы привести соответствующие технические параметры доступа к КИС.

6.1.4.6 Порядок определения подтверждающего доступ в заявке на предоставление доступа к ИР приведен в таблице 1.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Таблица 1 – Порядок определения подтверждающего доступ в заявке на предоставление доступа к ИР

№ п/п	Пользователь	Категория УЗ по назначению	Подтверждающий доступ	Условие применения
1	2	3	4	5
1	Работник ООО «ПТП»	Пользовательская, административная	Руководитель подразделения работника ООО «ПТП»	–

6.1.4.7 Очередь согласования заявки на предоставление доступа к ИР приведена в таблице 2.

6.1.4.8 Для определения разрешающего доступ следует использовать утвержденную МРиП ИС.

При отсутствии утвержденной МРиП ИС разрешающим доступ является руководитель структурного подразделения, являющегося функциональным заказчиком ИС.

Таблица 2 – Очередь согласования заявки на предоставление доступа к ИР

№ п/п	Пользователь	Категория УЗ по назначению	Список согласующих
1	2	3	4
1	Работник ООО «ПТП»	Пользовательская/ Административная	Руководитель подразделения работника ООО «ПТП» Начальник СБ Начальник ОИТиС

6.1.4.9 В процессе согласования заявки:

- Руководитель подразделения работника ООО «ПТП» проверяет обоснование необходимости и срок предоставления доступа к ИР;
- начальник СБ контролирует корректность назначения прав и полномочий доступа к ИР в соответствии с требованиями настоящего документа и других нормативных документов ООО «ПТП» в области ИБ по направлению деятельности СБ;
- начальник ОИТиС проверяет объем полномочий предоставления доступа к ИР.

6.1.4.10 Заявка на предоставление доступа к ИР должна быть подписана (при оформлении на бумажном носителе) подтверждающим доступ.

6.1.5 После выполнения заявки заявитель получает уведомление о результатах выполнения в СЭД или по электронной почте.

6.2 Прекращение доступа

6.2.1 Прекращение доступа ко всем ИР осуществляется на основании:

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

а) истечения срока действия УЗ, указанного в ранее оформленной заявке на предоставление доступа;

б) кадрового уведомления о прекращении трудового договора с работником ООО «ПТП»;

в) Положение о защите коммерческой тайны ПАО «Транснефть» и иной конфиденциальной информации ОР-03.100.00-КТН-061-19 (раздел 7);

г) заявки, оформленной в СЭД в соответствии с А.4 (приложение А), с выбором опции «Прекращение доступа ко всем информационным ресурсам».

6.2.2 Прекращение доступа к отдельным ИР осуществляется на основании заявки, оформленной в соответствии с А.4 (приложение А) с выбором опции «Прекращение доступа к нижеперечисленным информационным ресурсам».

6.2.3 Заявку на прекращение доступа к ИР оформляет заявитель в порядке, установленном настоящим пунктом.

6.2.3.1 Определяет способ оформления заявки (СЭД или на бумажном носителе) согласно 6.1.4.1.

6.2.3.2 При оформлении заявки в СЭД заявитель в электронном виде заполняет обязательные поля с последующим направлением заявки на согласование.

6.2.3.3 При оформлении заявки на бумажном носителе заявитель заполняет заявку в соответствии с А.4 (приложение А).

Для выбора необходимой роли ИС заявитель использует актуальную МРиП ИС, ссылка на которую приведена в перечне ИС. При отсутствии утвержденной МРиП ИС заявитель указывает перечень полномочий в ИС, доступ к которым требуется прекратить.

При оформлении заявки не допускается использование формулировки «прекращение доступа ко всем ИР кроме указанных ИР».

6.2.3.4 Заявка на прекращение доступа к ИР должна быть подписана (согласована при оформлении в СЭД) руководителем подразделения. Других согласований заявки на прекращение доступа к ИР не требуется.

6.2.3.5 Порядок определения, подтверждающего доступ в заявке на прекращение доступа к ИР приведен в таблице 3.

6.2.4 Прекращение доступа, оформленного в СЭД, осуществляется через СЭД (при прекращении трудового договора с работником ООО «ПТП»).

6.2.5 После выполнения заявки заявитель получает уведомление о результатах выполнения в СЭД или по электронной почте.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Таблица 3 – Порядок определения, подтверждающего доступ в заявке на прекращение доступа к ИР

№ п/п	Пользователь	Категория УЗ по назначению	Подтверждающий доступ	Условие применения
1	2	3	4	5
1	Работник ООО «ПТП»	Пользовательская, административная	Руководитель подразделения работника ООО «ПТП»	–

6.2.6 При прекращении доступа ко всем ИР (см. п. 6.2.1) администраторы УЗ в ИС должны обеспечить блокирование либо удаление (при отсутствии возможности блокирования) всех УЗ с даты, следующей за датой увольнения работника, либо с даты, указанной в заявке на прекращения доступа к ИР. При наличии технической возможности в ИС, администратор УЗ должен переименовать заблокированную УЗ с указанием «заблокирована» и даты блокировки в формате ДД.ММ.ГГГГ.

6.3 Пересмотр прав доступа

6.3.1 Процедура пересмотра прав доступа обеспечивает контроль и приведение предоставленных УЗ прав доступа к ролям ИС в соответствие с фактическими потребностями и требованиями ИБ.

6.3.2 Пересмотр прав доступа работников ООО «ПТП» для всех типов УЗ должен проводиться на регулярной основе с определенной для каждой ИС в перечне ИС периодичностью.

6.3.3 Процедуру пересмотра прав доступа для ИС, инициирует руководитель сотрудника путем формирования заявок в СЭД на утверждение актуальных и отклонение избыточных ролей пользователя ИС. Доступ пользователя по отклоненным заявкам автоматически прекращается.

При обнаружении предоставленных прав доступа, не соответствующих текущим должностным обязанностям кого-либо из работников, руководитель структурного подразделения ООО «ПТП» в срок не позднее 5 рабочих дней обеспечивает оформление соответствующих заявок на прекращение доступа к ИР ООО «ПТП» согласно настоящему документу (см. п. 6.2.2).

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

7 Управление документами

7.1 Перечень информационных систем

7.1.1 Разработка, согласование, утверждение

7.1.1.1 В ООО «ПТП» должен быть сформирован и поддерживается в актуальном состоянии перечень ИС.

7.1.1.2 Перечень ИС разрабатывает ОИТиС. Форма перечня ИС приведена в приложении В.

7.1.1.3 Перечень ИС должен быть согласован с начальником ОИТиС, начальником СБ и утвержден главным инженером.

7.1.2 Актуализация, хранение

7.1.2.1 Основаниями для внесения изменений в перечень ИС являются:

- для эксплуатируемых ИС – организационно-распорядительный документ на ввод ИС в промышленную/опытную эксплуатацию;
- для планируемых к внедрению ИС – договор на создание ИС или положительное заключение ОИТиС на заявку о создании ИС.

7.1.2.2 Ответственный за размещение информации по доступу на основании документов, указанных в п. 7.1.2.1, не позднее 2 рабочих дней размещает актуализированный перечень ИС и МРиП ИС (при включении ИС в перечень ИС).

7.1.2.3 Актуальный перечень ИС должен быть расположен на файловом сервере в разделе «Доступ к информационным ресурсам».

7.2 Матрица ролей и полномочий

7.2.1 Разработка, согласование, утверждение

7.2.1.1 МРиП ИС должна содержать раздел «Бизнес-роли» и раздел «Роли обслуживающего персонала».

Обязательные поля для разделов «Бизнес-роли» и «Роли обслуживающего персонала»:

- наименование роли;
- описание роли (при необходимости);
- административные полномочия (да, нет);
- обладатель информации;
- разрешающий доступ;
- лица, согласующие доступ (при необходимости);
- техническое описание (описание полномочий роли, включая тип и вид УЗ (если роль необходимо предоставлять УЗ, отличной от основной УЗ), а также все необходимые права

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

доступа, например, членство в группах доступа, права доступа к ФР, публикация ярлыков приложений на терминальных серверах или наименование роли из документа с описанием ролей и полномочий ИС, другое).

Обязательные поля для раздела «Роли обслуживающего персонала»:

- тип УЗ (локальная, доменная (с указанием допустимых доменов), ИС (СУБД));
- вид УЗ по назначению (административная, пользовательская, технологическая).

7.2.1.2 Форма МРиП ИС приведена в приложении Г.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Приложение А

(обязательное)

Формы заявок

А.1 Форма заявки на изменение параметров учетной записи

Заявка на изменение параметров учетной записи

В связи с *указать причину изменения параметров учетной записи с приложением обосновывающего документа (приказ/письмо)¹⁾* прошу выполнить изменение параметров учетной записи (без изменения прав доступа) во всех информационных системах у работника

И.О. Фамилия полностью		Информация о работнике		
Текущие параметры (которые необходимо изменить)	Новые параметры (на которые необходимо изменить)	Должность	Подразделение полностью	Контактные данные (e-mail, телефон)
1	2	3	4	5

Руководитель подразделения

должность, подразделение, И.О. Фамилия

Указать И.О. Фамилию, телефон заявителя

¹⁾ Указания по заполнению приведены курсивом.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

А.2 Форма заявки на создание или продление срока действия ФР-ресурса

Заявка на создание/продление срока действия файлового ресурса

В связи с _____ указать обоснование
 необходимости создания/продления¹⁾ _____

- 1 Краткое описание цели создания: _____
- 2 Предназначен для обмена информацией с работниками:

- 3 Размещение сведений с ограничительными грифами («К» и/или «КТ»): _____
- 4 Дата, до которой действует ресурс (не более 5 лет): _____
- 5 Подразделение: _____
- 6 Должности и И.О. Фамилии, разрешающих доступ: _____
- 7 Наименование ресурса: _

Приложение (при необходимости): Структура ресурса и роли доступа на ___ листах.

Руководитель подразделения

 должность, подразделение, организация, И.О.
 Фамилия

СОГЛАСОВАНО
 Начальник ОИТиС

_____ И.О. Фамилия

Начальник службы безопасности

_____ И.О. Фамилия

Указать И.О. Фамилию, телефон заявителя

¹⁾Здесь и далее указания по заполнению приведены курсивом.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Приложение

Структура ресурса

Указать наименование ресурса (заполняется обязательно)

(Информация ниже заполняется при необходимости)

Указать наименование папки 1

Указать наименование папки 1.1

Указать наименование папки 1.1.1

Указать наименование папки 1.1.2

...

Указать наименование папки 1.1.N

Указать наименование папки 1.2

Указать наименование папки 1.2.1

Указать наименование папки 1.2.2

...

Указать наименование папки 1.2.N

...

Указать наименование папки 1.N

...

Указать наименование папки N

Указать наименование папки N.1

...

...

2 Роли доступа

п/п	Наименование роли	Описание роли
	2	3
	Указать наименование роли 1	Указать описание роли, например: доступ на «чтение» содержимого папки 1.1.1 и всех папок внутри папки 1.1.1
	Указать наименование роли 2	Указать описание роли, например: доступ на «запись» содержимого папки 1.1.1 и всех папок внутри папки 1.1.1

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

А.3 Форма заявки на предоставление доступа к ИР

Регистратору заявок

Заявка на предоставление доступа к информационным ресурсам

В _____ указать обоснование необходимости предоставления прав доступа, связи с _____
указать реквизиты договора или иного документа, обосновывающего предоставление доступа, срок действия договора (заполняется только для работников сторонней организации) ¹⁾
прошу для работника(ов):

п/п	И.О Фамилия (полностью)	Дол жность	Подразделе ние полностью (отдел/служба, управление, департамент и т. п.)	Контактные данные (e-mail, телефон, офис, кабинет)	Учетная запись (при наличии)
	2	3	4	5	6

Заполняется при необходимости создания учетной записи (УЗ)

создать УЗ со следующими параметрами:

Предлагаемое имя: _____ *заполняется только для технологических, тестовых, групповых УЗ*

Пользовательская Административная Тестовая

Информационной системы _____ *указать наименование ИС из перечня ИС*

Способ передачи учетных данных (логин, пароль):

Очно Дистанционно

Заполняется при необходимости установки:

Персонального компьютера

Программного обеспечения _____ *указать наименование программного обеспечения*

предоставить доступ к следующим информационным ресурсам:

Наименован ие информационной системы	Наименовани е роли в информационной системе	Наименов ание и параметры информационного ресурса	Срок предоставления доступа к информационному ресурсу	Разреш ающий доступ (должн ость, И.О. Фамилия)
1	2	3	4	5
<i>Указать наименование информационной системы из перечня информационных систем</i>	<i>Указать наименование роли из матрицы ролей и полномочий информационной системы</i>	<i>Указать наименование информационного ресурса и дополнительную информацию (при необходимости)</i>	<i>Указать срок, но не более срока действия учетной записи</i>	<i>Указа ть разреш ающего доступ из матрицы ролей и полномочий</i>

¹⁾ Здесь и далее указания по заполнению приведены курсивом.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Подтверждающий доступ

 должность, подразделение, И.О. Фамилия

СОГЛАСОВАНО

Начальник службы безопасности ООО «ПТП»

_____ И.О. Фамилия

Начальник ОИТиС ООО «ПТП»

_____ И.О.
 Фамилия

Указать И.О. Фамилия, телефон заявителя

Указания по заполнению:

А.3.1 В заявке должны быть заполнены все поля.

А.3.2 Указанные в заявке работники являются ответственными за использование предоставленных им учетных записей.

А.3.3 Заявка может быть оформлена на несколько работников, если доступ к информационным ресурсам для одного типа учетной записи.

А.3.4 В графе 6 приводят контактные данные пользователя. При установке персонального компьютера или программного обеспечения указывают расположение рабочего места пользователя.

А.3.5 В графе 7 приводят учетную запись пользователя с указанием домена (при наличии), например, FamiliyaIO@ak.tn.corp.

А.3.6 Разделы по созданию учетных записей и установки персонального компьютера/программного обеспечения (обведены рамкой) заполняют при необходимости либо удаляют из заявки.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

А.4 Форма заявки на прекращение доступа к ИР

Регистратору заявок

Заявка на прекращение доступа к информационным ресурсам

В связи с _____ в _____
указать обоснование необходимости и дату прекращения прав доступа¹⁾
прошу для работника(ов):

/п	И. О. Фамилия полностью	Должность	Подразделение полностью	Контактные данные (при наличии)	Учетная запись (при выборе опции «прекращение доступа к нижеперечисленным информационным ресурсам»)
	2	3	4	5	6

прекратить доступ (выбрать одно из значений)

ко всем информационным ресурсам и заблокировать все учетные записи, за исключением технологических, ответственным за использование которых является работник(и)

к нижеперечисленным информационным ресурсам:

Наименование информационной системы	Наименование роли информационной системы
1	2
<i>Указать наименование информационной системы из перечня информационных систем</i>	<i>Указать наименование роли из матрицы ролей и полномочий информационной системы</i>

Подтверждающий доступ

должность, подразделение, И.О. Фамилия

Указать И.О. Фамилия, телефон заявителя

¹⁾ Здесь и далее указания по заполнению приведены курсивом.

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Приложение Б

(обязательное)

Передача учетных данных

Б.1 Общие требования к передаче учетных данных

Б.1.1 Формирование учетных данных (имя УЗ и пароль) любой категории УЗ (см. 5.2.2) осуществляется администратором УЗ в соответствии с требованиями настоящего документа.

Б.1.2 Передачу работникам учетных данных любой категории УЗ (см. 5.2.2) осуществляет администратор УЗ очно или дистанционно.

Б.1.3 Если требуется сменить (сбросить) пароль основной УЗ работника ООО «ПТП», когда работник не имеет возможности идентифицировать свою личность, кроме очного получения пароля, разрешается любому лицу из его структурного подразделения (с указанием причины сброса пароля) обращаться по корпоративной электронной почте в ОИТиС, при этом пароль будет направлен SMS–сообщением на номер мобильного телефона работника, которому сбрасывают пароль, указанного при обращении в ОИТиС.

Б.1.4 Работник обязан сменить пароль при первом его использовании.

Б.1.5 Ответственность за ознакомление с выписками из нормативных документов по парольной и антивирусной защите при передаче учетных данных дистанционным способом несет сам работник.

Б.1.6 Ответственность за организацию допуска работника к информационным ресурсам несет его руководитель.

Б.2 Способы передачи учетных данных

Б.2.1 Очно

Учетные данные передаются лично в руки работнику в запечатанном конверте. Если учетные данные передает администратор, лично создавший УЗ/сбросивший пароль для УЗ, допускается их передача без конверта.

Б.2.2 Дистанционно (с использованием каналов передачи данных)

а) При передаче учетных данных первой пользовательской доменной УЗ (УЗ должна быть заблокирована), для которой еще отсутствует адрес электронной почты в корпоративной почтовой системе, на рабочую (в случае отсутствия - на личную) электронную почту, указанную в заявке работника, направляется имя УЗ (логин), выписки из нормативных документов ООО «ПТП» с требованиями по парольной и антивирусной защите. Передача первоначального пароля указанной УЗ осуществляется на служебный или личный номер мобильного телефона работника, указанный в заявке, путем направления SMS–сообщения.

б) Для информационных систем, которые обеспечивают возможность принудительной смены пароля УЗ при первом использовании, учетные данные направляются на корпоративную

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

электронную почту или на электронную почту, на которую обеспечена возможность передачи конфиденциальной информации. Если информационная система не обеспечивает такой возможности, передача учетных данных осуществляется на служебный или личный номер мобильного телефона работника, указанный в заявке, путем направления SMS–сообщения.

Приложение В
(рекомендуемое)
Форма перечня информационных систем

№ п/п	Полное наименование	Краткое наименование	Функциональный заказчик	Курирующее подразделение департамента информационных технологий	Ссылка на матрицу ролей и полномочий	Периодичность пересмотра прав доступа
1	2	3	4	5	6	7

ООО «ПТП»

Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»

П-21-ПТП-015-20

Приложение Г
(рекомендуемое)
Форма матрицы ролей и полномочий информационной системы
Матрица ролей и полномочий ИС _____

Раздел «Бизнес-роли» (обязательный раздел)

№ п/п	Наименование роли	Описание роли	Административные полномочия	Наименование информационного ресурса	Обладатель информации ²⁾	Разрешающий доступ ²⁾	Лица, согласующие доступ (при необходимости) ²⁾	Техническое описание (определяется в зависимости от реализации информационной системы)
1	2	3	4	5	6	7	8	9

Раздел «Роли обслуживающего персонала» (обязательный раздел)

№ п/п	Наименование роли	Описание роли	Административные полномочия	Обладатель информации	Разрешающий доступ	Лица, согласующие доступ (при необходимости)	Техническое описание (определяется в зависимости от реализации информационной системы)	Тип учетной записи (доменная (с указанием допустимых доменов), локальная, информационной системы)	Категория учетной записи по назначению (административная, пользовательская, технологическая)
1	2	3	4	5	6	7	8	9	10

Указания по заполнению

1) Рекомендуется использовать файлы данных в виде электронных таблиц (формат xls, xlsx и др.).

ООО «ПТП»

Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»

П-21-ПТП-015-20

2) Если одну роль можно использовать для доступа ко многим информационным ресурсам («организационным наборам», «заводам» и т. п.), рекомендуется графы «Наименование роли», «Обладатель информации» и «Разрешающий доступ», «Лица, согласующие доступ (при необходимости)» разместить в отдельной таблице (на отдельном листе электронных таблиц).

3) Техническое описание полномочий роли или наименование роли из документа с описанием ролей и полномочий информационной системы, а также все необходимые права доступа, например, членство в группах доступа, права доступа к файловым ресурсам, публикация ярлыков приложений на терминальных серверах.

4) В графе «административные полномочия» указывают либо «да», либо «нет».


ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

ООО «ПТП»	Положение о порядке управления доступом к информационным ресурсам ООО «ПТП»	П-21-ПТП-015-20
-----------	---	-----------------

Библиография

[1] Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

Разработал
Начальник отдела ИТ и С



М.Б. Балаш