

АКЦИОНЕРНОЕ ОБЩЕСТВО  
«ЗАРУБЕЖНЕФТЬ»

УТВЕРЖДАЮ  
Заместитель Генерального директора  
по экономике и финансам  
Д.Н. Максимов

ИНСТРУКЦИЯ  
ПО УПРАВЛЕНИЮ УЧЕТНЫМИ ЗАПИСЯМИ ДОСТУПА  
К ИНФОРМАЦИОННЫМ РЕСУРСАМ

№ ИН ОБ-09.0-01  
РЕДАКЦИЯ 2.00

(взамен Инструкции по управлению учетными записями доступа к информационным ресурсам,  
№ ИН ОБ-09.0-01, редакция 1.00, утвержденной приказом от 13.11.2017 № 330)

Идентификатор документа (ELMA Id: aee45c65-7eac-435f-8915-c1f9f15d8572) Документ подписан		
Владелец сертификата: организация, сотрудник	Сертификат: серийный номер, период действия	Дата и время подписания
МАКСИМОВ ДЕНИС НИКОЛАЕВИЧ,	057880900065B1DDA44DB8B29B7AFEEF74, с 03.05.2024 11:41 по 03.05.2025 11:46	19.07.2024 10:51 Подпись соответствует файлу документа

Москва  
2024

## ОГЛАВЛЕНИЕ

I. ОБЩИЕ ПОЛОЖЕНИЯ .....	3
II. СХЕМА ПРОЦЕДУРЫ УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ .....	4
III. КЛЮЧЕВЫЕ ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ .....	5
3.1. Администраторы доступа к информационным ресурсам .....	5
3.2. Профили доступа информационных ресурсов .....	5
3.3. Порядок создания и изменения учетных записей .....	6
3.4. Порядок блокировки учетных записей .....	7
3.5. Порядок предоставления расширенных полномочий .....	8
Приложение № 1 .....	9
Приложение № 2 .....	11
Приложение № 3 .....	13
Приложение № 4 .....	14
Приложение № 5 .....	16

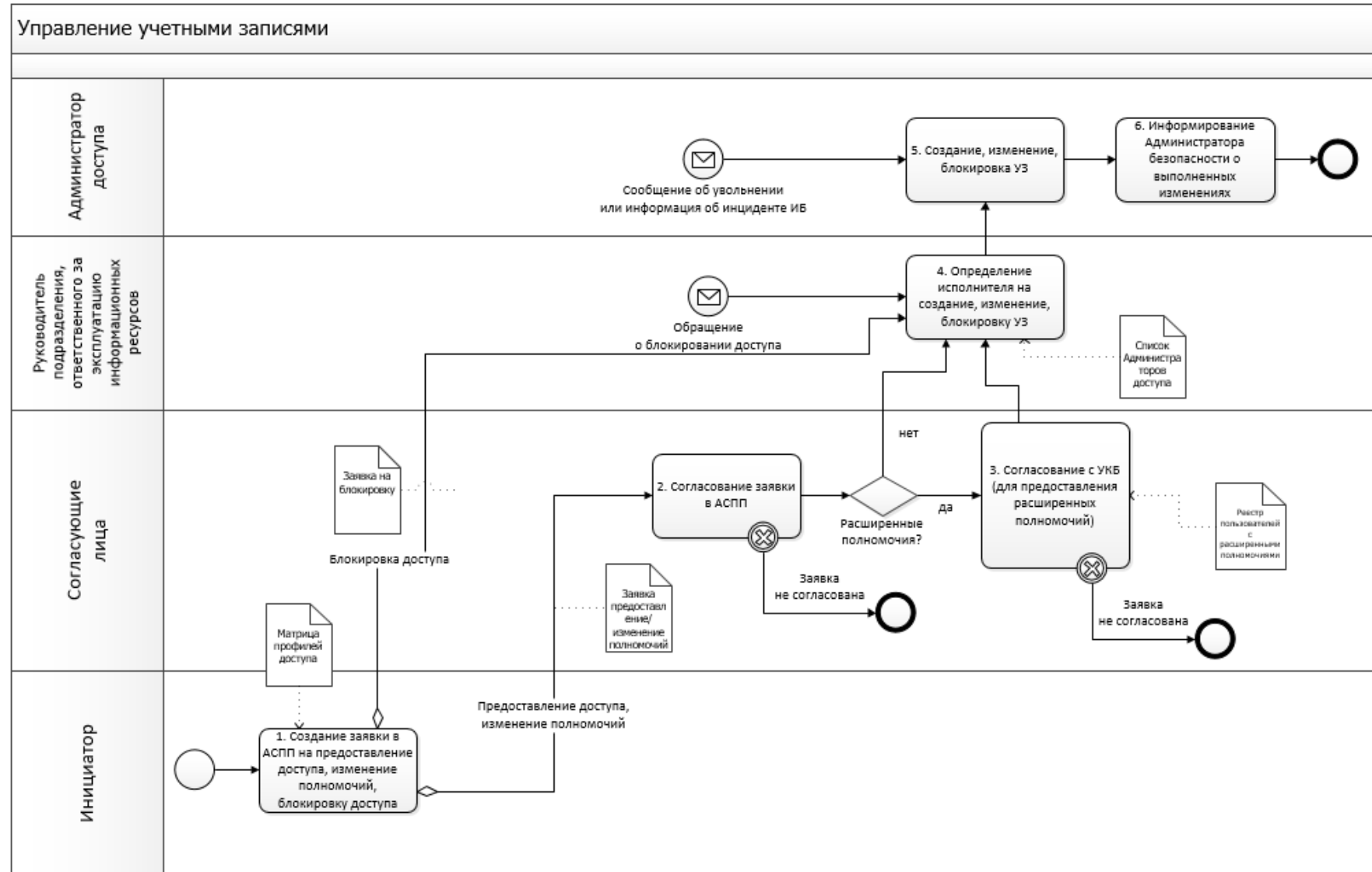
## I. ОБЩИЕ ПОЛОЖЕНИЯ

Наименование документа	Инструкция по управлению учетными записями доступа к информационным ресурсам	
<b>Регламентируемый бизнес-процесс / подпроцесс. Степень покрытия бизнес-процесса документом (полностью / частично)</b>	Бизнес-процесс Об-9 «Управление информационными технологиями». Детализирует процедуру управления учетными записями подпроцесса «5. Управление поддержкой и обслуживанием»	
<b>Период действия (постоянный / до)</b>	Постоянный	
<b>Внешние законодательные требования, требования политик, стратегических документов</b>	<ul style="list-style-type: none"> <li>– Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи»;</li> <li>– Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;</li> <li>– Политика информационной безопасности АО «Зарубежнефть»</li> </ul>	
<b>Область действия / степень распространения требований на ДО</b>	АО «Зарубежнефть»	Полностью
	ГриД	-
	НиС	-
	Сервисы	-
	Прочие	-
<b>Разработчик документа, должность, ФИО, контакты (e-mail, телефон)</b>	<p>Данник Давид Вахтангович, главный специалист, Управление информационных технологий, т. 30-71, e-mail: ddannik@nestro.ru;</p> <p>Кузнецов Дмитрий Владимирович, руководитель направления, отдел информационной безопасности Центра обслуживания бизнеса АО «Зарубежнефть», т. 84-57, e-mail: dvkuznetsov@nestro.ru</p>	

Инструкция устанавливает порядок создания, изменения и блокировки учетных записей служб каталогов, ресурсов информационных систем, хранилищ конфигураций, серверов баз данных, внутренних и внешних веб-сервисов, используемых в АО «Зарубежнефть» (далее – Общество) и дочерних обществах АО «Зарубежнефть» (далее – ДО).

## II. СХЕМА ПРОЦЕДУРЫ УПРАВЛЕНИЯ УЧЕТНЫМИ ЗАПИСЯМИ ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Система условных обозначений (нотация), используемая в схеме процедуры приведена в Приложении № 1 к настоящей инструкции.



### **III. КЛЮЧЕВЫЕ ТРЕБОВАНИЯ К ВЫПОЛНЕНИЮ**

#### **3.1. Администраторы доступа к информационным ресурсам**

3.1.1. С целью определения ответственных лиц за фактическое предоставление доступа для каждого информационного ресурса определяются Администраторы доступа.

3.1.2. Список Администраторов доступа с указанием: фамилии имени отчества, должности, телефона, адреса электронной почты, имени компьютера по каждому информационному ресурсу создается и актуализируется подразделениями, ответственными за сопровождение информационных ресурсов либо кураторами договоров на сопровождение информационных ресурсов (в случае отсутствия отдельного подразделения по сопровождению информационного ресурса). Сведения по администраторам доступа после их формирования или актуализации направляются подразделениями, ответственными за сопровождение информационных ресурсов, в отдел информационной безопасности Центра обслуживания бизнеса АО «Зарубежнефть» (далее – ОИБ) для последующего свода информации и работы со сводным списком.

#### **3.2. Профили доступа информационных ресурсов**

3.2.1. Профили доступа предназначены для определения predetermined наборов разрешенных действий (ролей), содержащих права доступа к функциональным возможностям и данным информационных ресурсов.

3.2.2. Для каждой учетной записи определяется набор профилей доступа к информационному ресурсу. Роль считается разрешенной для учетной записи, если она присутствует хотя бы в одном профиле доступа из набора.

3.2.3. Для целей определения набора информационных ресурсов, доступ к которым предоставляется при приеме на работу, определяется признак базового информационного ресурса.

3.2.4. Для определения набора полномочий по умолчанию, профиль доступа имеет признак отношения к базовому набору полномочий. У каждого информационного ресурса должен существовать один профиль с признаком базового набора полномочий.

3.2.5. Для целей контроля за особыми полномочиями пользователей профиль доступа имеет признак отношения к расширенному набору полномочий. Каждый информационный ресурс может иметь несколько профилей с признаками расширенных полномочий.

3.2.6. Состав профилей доступа информационных ресурсов определяется матрицей профилей доступа информационных ресурсов, которая содержит признаки базовых ресурсов, а также признаки базовых и расширенных полномочий.

3.2.7. Матрица профилей доступа информационных ресурсов создается, актуализируется и публикуется на Корпоративном портале АО «Зарубежнефть» в соответствии с установленной формой (Приложение № 3) Управлением информационных технологий АО «Зарубежнефть» (далее – УИТ).

3.2.8. Актуализация матрицы профилей доступа информационных ресурсов производится по мере необходимости, но не реже одного раза в год.

3.2.9. Матрица профилей доступа информационных ресурсов публикуется на общем информационном ресурсе, доступном Инициаторам (в АО «Зарубежнефть» – на корпоративном портале АО «Зарубежнефть» раздел ДОКУМЕНТЫ > ШАБЛОНЫ ДОКУМЕНТОВ > Шаблоны заявок).

3.2.10. По умолчанию доступ работников Общества и ДО к Интернет-ресурсам с их автоматизированного рабочего места заблокирован. Для получения разрешения работы с определенными Интернет-ресурсами, доступ к которым необходим для выполнения должностных обязанностей работника, оформляется обоснованная заявка в автоматизированной системе поддержки пользователей (далее – АСПП), которая согласовывается с УИТ и ОИБ.

3.2.11. Независимо от профиля доступа и разрешенных действий (ролей) пользователь при работе с информационными ресурсами и Интернет-ресурсами обязан соблюдать требования действующей Инструкции пользователя по обеспечению информационной безопасности, а также иных внутренних нормативных документов Общества или ДО.

3.2.12. Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей, определенные действующей Политикой управления доступом к ресурсам корпоративной сети.

### **3.3. Порядок создания и изменения учетных записей**

3.3.1. В общем случае создание или изменение учетных записей производится на основании заявки на предоставление доступа к информационным ресурсам, направленной в АСПП.

3.3.2. Создание учетных записей при приеме сотрудника на работу требующих обеспечения рабочего места средствами вычислительной техники и базовыми ИТ-сервисами, производится в АСПП или на основании служебной записки (Приложение № 4). В этом случае создаются учетные записи к информационным ресурсам, имеющим признак базового. Уровень доступа вновь принятого сотрудника к базовым информационным ресурсам определяется профилями базовых полномочий.

3.3.3. Процедура согласования заявок на предоставление доступа к информационным ресурсам осуществляется в АСПП в соответствии с Политикой управления доступом к ресурсам корпоративной сети.

3.3.4. Согласованная заявка направляется Администраторам доступа для организации доступа.

3.3.5. Создание или изменение учетной записи, связанной с электронной подписью (далее – ЭП), производится Администраторами доступа после завершения процедуры получения ЭП пользователем.

3.3.6. Создание или изменение учетной записи предполагает заполнение всех обязательных атрибутов учетной записи значениями, соответствующими требованиям заявки.

3.3.7. Допускается использование специализированных программных и аппаратных средств автоматизации процесса предоставления доступа при создании и изменении учетных записей, работа которых не противоречит Политике управления доступом к ресурсам корпоративной сети. Порядок создания и изменения учетных записей при использовании таких средств определяется эксплуатационной документацией этих средств.

3.3.8. Создание или внесение изменений в учетную запись пользователя Администратор доступа осуществляет в соответствии с действующей Политикой управления доступом к ресурсам корпоративной сети или сообщает о причине отказа.

#### **3.4. Порядок блокировки учетных записей**

3.4.1. Блокировка учетных записей пользователей осуществляется Администраторами доступа в следующих случаях:

- по инициативе владельца информационного ресурса;
- по инициативе руководителя структурного подразделения пользователя;
- по инициативе подразделения, ответственного за обеспечение функций безопасности (в АО «Зарубежнефть» – Управление корпоративной безопасности (далее – УКБ));
- по инициативе подразделения, ответственного за обеспечение функций информационной безопасности (в АО «Зарубежнефть» – ОИБ).

3.4.2. Блокировка учетных записей пользователей в штатном режиме осуществляется на основании обращений лиц, указанных в п. 3.4.1, во внештатном режиме (инцидент информационной безопасности) блокирование учетных записей пользователей, вовлеченных в инцидент информационной безопасности, может осуществляться оперативно, без обращений.

3.4.3. Блокировка учетных записей уволенных работников производится Администраторами доступа сразу после получения сообщения об увольнении в соответствии с порядком, определенным в Политике управления доступом к ресурсам корпоративной сети.

3.4.4. Администраторами доступа осуществляется инвентаризация учетных записей пользователей на предмет наличия учетных записей уволенных работников с целью их дальнейшей блокировки.

### **3.5. Порядок предоставления расширенных полномочий**

3.5.1. Фактом предоставления пользователю расширенных полномочий является назначение пользователю любого из профилей доступа с признаком расширенных полномочий.

3.5.2. Расширенные полномочия могут быть предоставлены только пользователям, входящим в реестр пользователей с расширенными полномочиями.

3.5.3. Реестр пользователей с расширенными полномочиями создается и актуализируется УИТ, согласовывается с УКБ и ОИБ, утверждается заместителем Генерального директора АО «Зарубежнефть», курирующим вопросы информационной безопасности. При согласовании УКБ проводит проверку пользователей с расширенными полномочиями в соответствии с действующим Регламентом о проведении проверки физических лиц.

3.5.4. В целях обеспечения контроля за использованием пользователями расширенных полномочий УИТ и ОИБ на постоянной основе проводится:

- анализ действий пользователей с расширенными полномочиями;
- инвентаризация и актуализация списка пользователей с расширенными полномочиями.

В случае фиксации факта нарушения Политики информационной безопасности пользователями с расширенными полномочиями выявившее подразделение информирует:



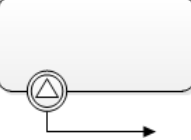









- в АО «Зарубежнефть» – УИТ, УКБ и ОИБ;
- в дочерних обществах – подразделение дочернего общества, ответственное за обеспечение функций корпоративной безопасности, УКБ и ОИБ.



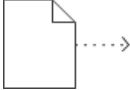
3.5.5. Постоянный аудит и контроль за использованием расширенных полномочий пользователями осуществляет ОИБ.



## НОТАЦИЯ СХЕМЫ ПРОЦЕДУРЫ

При разработке схемы процедуры использованы следующие обозначения нотации BPMN:

Обозначение	Описание
	Действие – общий термин, обозначающий работу, выполняемую исполнителем в ходе бизнес-процесса
	Подпроцесс. Указывает на то, что данное действие является подпроцессом. В данном случае детали находятся на нижнем уровне
	Поток исключений встречается за пределами стандартного потока операций. Основывается на промежуточных событиях, возникающих в ходе процесса. При наступлении промежуточного события, действие отменяется
	Шлюзы используются для контроля расхождений и схождений потока операций бизнес-процесса
	Поток операций служит для отображения того порядка, в котором организованы действия бизнес-процесса
	Условный поток операций. Поток операций может зависеть от условных выражений, оцениваемых согласно времени выполнения для того, чтобы определить, будет ли использоваться поток или нет
	Поток операций по умолчанию. Поток операций данного типа используется в том случае, если все остальные исходящие условные потоки операций не являются верными во время выполнения действия
	Поток сообщений служит для отображения обмена сообщениями между двумя участниками, готовыми эти сообщения отсылать и принимать
	Стартовое и конечное событие указывает на то, в какой точке берет начало и в какой точке завершится бизнес-процесс
	Передача сигнала между процессами. Один сигнал может обрабатываться многими получателями. Начальное, промежуточное и завершающее событие соответственно
	Получение сообщений
	Регулярные события, моменты времени, временные периоды и таймауты

Обозначение	Описание
	Генерация заданного типа ошибок
	Инициирование отмены действия
	Данные, используемые для отображения информации в информационных потоках, в т.ч. входящих, исходящих и изменяемых документов

## СПИСОК СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

### Термины и определения:

Термин	Определение
<b>Active Directory</b>	Служба каталогов корпорации Microsoft для операционных систем семейства Windows Server
<b>Администратор доступа</b>	Специалист, наделенный полномочиями осуществлять действия с учетными записями. Администратор доступа назначается руководителем подразделения, ответственным за эксплуатацию информационных ресурсов из числа сотрудников данного подразделения либо исполнителя, привлекаемого в рамках договорных отношений для поддержки эксплуатации соответствующего информационного ресурса. В исключительных случаях возможно назначение администратора доступа из числа сотрудников других структурных подразделений по согласованию с руководителем соответствующего структурного подразделения
<b>Аутентификация</b>	Процедура проверки принадлежности пользователя доступа предъявленного им идентификатора и подтверждение его подлинности
<b>Информационные ресурсы</b>	Информация и программно-технические средства, осуществляющие ее обработку, передачу и хранение с применением информационных технологий, в т.ч. файловые ресурсы, корпоративные средства групповой работы (эл.почта, календари, задачи), веб-порталы, корпоративные, локальные и внешние информационные системы, автоматизированные рабочие места
<b>Информационная система</b>	Совокупность программно-технических и других средств, используемых для хранения, обработки и передачи информации, с целью решения бизнес-задач подразделений Общества
<b>Информационная инфраструктура</b>	Система организационных структур, обеспечивающих функционирование и развитие информационного пространства Общества и средств информационного взаимодействия. Информационная инфраструктура включает совокупность информационных центров, банков данных и знаний, систем связи и обеспечивает доступ потребителей к информационным ресурсам
<b>Инициатор</b>	Руководитель подразделения, инициирующего процедуру создания, изменения или блокировку учетной записи

<b>Термин</b>	<b>Определение</b>
<b>Владелец информационного ресурса</b>	Структурное подразделение, ответственное за согласование предоставления доступа к информационному ресурсу или информационной системе, ассоциированной с информационным ресурсом
<b>Владелец информационной системы</b>	Структурное подразделение, ответственное за регламентацию процессов, автоматизированных с помощью этой информационной системы, формирование отчетных форм и документов информационной системы, наполнение и изменение справочников
<b>Реестр расширенных полномочий</b>	Документ, содержащий перечень пользователей, обладающих полномочиями администратора на рабочих станциях корпоративной сети и/или правами администратора информационных ресурсов
<b>Согласующие лица</b>	Лица, участвующие в согласовании доступа пользователей к информационным ресурсам
<b>Структурное подразделение, ответственное за сопровождение информационных ресурсов</b>	Структурное подразделение, осуществляющее настройку, обновление, поддержание в работоспособном состоянии, управление правами пользователей в информационных системах и ИТ-сервисах (для АО «Зарубежнефть» - Управление развития и сопровождения информационных систем Центра обслуживания бизнеса)
<b>Учетная запись</b>	Хранимая в информационной системе совокупность данных о пользователе, необходимая для его аутентификации и предоставления доступа

**Список сокращений:**

<b>Сокращение</b>	<b>Полное наименование</b>
<b>АСПП</b>	Автоматизированная система поддержки пользователей
<b>ДО</b>	Дочернее общество АО «Зарубежнефть»
<b>ИС</b>	Информационная система
<b>Общество</b>	АО «Зарубежнефть»
<b>ОИБ</b>	Отдел информационной безопасности Центра обслуживания бизнеса АО «Зарубежнефть»
<b>УИТ</b>	Управление информационных технологий АО «Зарубежнефть»
<b>УКБ</b>	Управление корпоративной безопасности АО «Зарубежнефть»
<b>ЭП</b>	Электронная подпись

Приложение № 3  
к Инструкции по управлению  
учетными записями доступа к  
информационным ресурсам

### Матрица профилей доступа информационных ресурсов

№ п/п	Информационный ресурс	Владелец ресурса	Признак базового ресурса	Профиль	Признак базовых полномочий	Признак расширенных полномочий
1.	Ресурс 1	Владелец ресурса 1	+	Профиль 1	+	
				Профиль 2		+
				Профиль 3		
2.	Ресурс 2	Владелец ресурса 2		Профиль 1	+	
				Профиль 2		+
				Профиль 3		+
...						

Приложение № 4  
к Инструкции по управлению  
учетными записями доступа к  
информационным ресурсам

*Должность руководителя  
структурного подразделения,  
ответственного за безопасность  
в дательном падеже  
(в АО «Зарубежнефть» – УКБ)  
Фамилия И.О. руководителя в  
дательном падеже*

*Должность руководителя  
структурного подразделения,  
ответственного за  
сопровождение  
информационных ресурсов в  
дательном падеже  
Фамилия И.О. руководителя в  
дательном падеже*

## СЛУЖЕБНАЯ ЗАПИСКА

В связи с приемом на работу или иное должность ФИО сотрудника (ПОЛНОСТЬЮ) в отдел/управление на период с/по или на период действия трудового договора прошу Вас:

1. Предоставить **ПОСТОЯННЫЙ** пропуск в здание Общества и обеспечить:

☐ получение/сдачу ключей от кабинета(-ов) *укажите номер (-а) кабинета (-ов);*

☐ доступ по пропуску в кабинет(-ы) *укажите номер (-а) кабинета (-ов).*

**\* Выдача ключей осуществляется только сотрудникам Общества. Для всех остальных необходимо в установленном порядке направить в Управление корпоративной безопасности докладную записку с указанием обоснования.**

2. Обеспечить рабочее место в кабинете № *номер кабинета* средствами вычислительной техники (СВТ в наличии на рабочем месте – *ДА/НЕТ*) и обеспечить базовыми ИТ сервисами:

- учетная запись сотрудника для аутентификации и авторизации (*укажите написание имени и фамилии в латинице как в загранпаспорте*);
- подключение к каталогу общего доступа подразделения (*ДА/НЕТ*);
- электронная почта (*ДА/НЕТ*);
- доступ к ресурсам сети Интернет (*ДА/НЕТ*);
- подключение к сервису централизованной печати (*ДА/НЕТ*);
- фиксированная телефонная связь:

а) внутренняя телефонная связь: *ДА/НЕТ;*

б) доступ на междугородние линии связи: *ДА/НЕТ;*

в) доступ на международные линии связи: *ДА/НЕТ;*

Дата приема сотрудника на работу: *Дата.*

Непосредственным руководителем данного сотрудника будет являться:

*укажите ФИО непосредственного руководителя.*

*Должность руководителя подразделения*

*И.О. Фамилия*

Фамилия, имя, отчество исполнителя  
Структурное подразделение, должность  
Телефон  
Электронная почта

**Ключевые вопросы к Инструкции по управлению учетными  
записями доступа к информационным ресурсам**

1. Какие типы учетных записей определены в настоящей инструкции?
2. Что такое профиль доступа?
3. Какие функции выполняет Администратор доступа?
4. В каких случаях возможна блокировка учетных записей?
5. Каким пользователям могут быть предоставлены расширенные полномочия?