

АКЦИОНЕРНОЕ ОБЩЕСТВО  
«ЗАРУБЕЖНЕФТЬ»

Приложение № 1

УТВЕРЖДЕНА  
приказом АО «Зарубежнефть»  
от «17» июня 2021 г. № 124

**ПОЛИТИКА**  
**УПРАВЛЕНИЯ ДОСТУПОМ**  
**К РЕСУРСАМ КОРПОРАТИВНОЙ СЕТИ**

№ ПТ ОБ-09.5-07  
РЕДАКЦИЯ 2.00

Москва  
2021

**ОГЛАВЛЕНИЕ**

|  |    |
|--|----|
| I. ОБЩИЕ ПОЛОЖЕНИЯ .....                                       | 3  |
| II. ОБЩИЕ СВЕДЕНИЯ .....                                       | 3  |
| 2.1. Условия применения .....                                  | 3  |
| III. ПРЕДОСТАВЛЕНИЕ ДОСТУПА К РЕСУРСАМ КОРПОРАТИВНОЙ СЕТИ..... | 4  |
| 3.1. Порядок предоставления доступа .....                      | 4  |
| 3.2. Порядок изменения доступа .....                           | 4  |
| 3.3. Кадровые перемещения .....                                | 5  |
| IV. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УДАЛЕННОГО ДОСТУПА.....             | 5  |
| 4.1. Общая информация.....                                     | 5  |
| 4.2. Требования к организации удаленного доступа .....         | 6  |
| V. ПАРОЛЬНАЯ ПОЛИТИКА .....                                    | 7  |
| 5.1. Общие требования .....                                    | 7  |
| 5.2. Требования к сложности паролей.....                       | 7  |
| 5.3. Ограничения .....   | 7  |
| VI. КОНТРОЛЬ .....   | 8  |
| VII. ОТВЕТСТВЕННОСТЬ.....                                      | 9  |
| Приложение № 1 .....   | 10 |
| Приложение № 2 .....   | 12 |

## I. ОБЩИЕ ПОЛОЖЕНИЯ

| Наименование документа   | Политика управления доступом к ресурсам корпоративной сети  |           |
|--|---|-----------|
| Регламентируемый бизнес-процесс / подпроцесс   | Об-9 Управление информационными технологиями / Об-9.5 Информационная безопасность   |           |
| Степень покрытия бизнес-процесса документом:<br>– полностью;<br>– частично (указать область покрытия)                                    | Частично (в части управления доступом к информационным ресурсам)  |           |
| Период действия (постоянный / до)  | Постоянный  |           |
| Внешние законодательные требования, требования политик, стратегических документов  | Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».<br>Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» |           |
| Область действия / степень распространения требований на ДО:<br>(указываются только предприятия, на которые распространяются требования) | АО «Зарубежнефть»   | Полностью |
|  | ГриД  | Полностью |
|  | НиС   | Полностью |
|  | Сервисы   | Полностью |
|  | Прочие  | -         |
| Разработчик документа, должность, ФИО, контакты (e-mail, телефон)  | УИТ: Данник Давид Вахтангович, главный специалист, т. 30-71, e-mail: DDannik@nestro.ru  |           |

## II. ОБЩИЕ СВЕДЕНИЯ

### 2.1. Условия применения

Настоящий документ предназначен для установления единых норм, правил и процедур, необходимых для реализации мер управления доступом.

С целью обеспечения защиты информационных ресурсов от их незаконного использования, утечки сведений конфиденциального характера, умышленного или неосторожного нарушения целостности или доступности критичной информации и других

угроз информационной безопасности настоящая Политика управления доступом к ресурсам корпоративной сети (далее – Политика) устанавливает единый порядок предоставления, изменения и отмены доступа пользователей к ресурсам корпоративной сети и соответствующие требования безопасности.

Доступ к ресурсам корпоративной сети должен осуществляться зарегистрированными пользователями при предъявлении доказательств (логин и пароль) их подлинности (аутентификации). Используемая схема аутентификации должна применять шифрование для обмена ключевой информацией.

В случае предоставления работникам Общества, дочерних обществ и другим лицам доступа к ресурсам корпоративной сети, должна осуществляться процедура их регистрации в качестве пользователей корпоративной сети, в результате которой для каждого работника создается одна или в особых случаях несколько доменных УЗ, используемых для получения доступа к локальному компьютеру, сетевым сервисам, разделяемым сетевым файловым ресурсам (файлы, каталоги, диски, рабочие станции, периферия), серверам баз данных и другим ИС (далее – доступ к ИС), доступ к которым возможно предоставлять путём доменной аутентификации.

В случае невозможности разграничения доступа средствами доменной аутентификации, следует создавать локальные учетные записи.

Не допускается использование пользователями чужих учётных записей для осуществления доступа к ресурсам корпоративной сети.

### **III. ПРЕДОСТАВЛЕНИЕ ДОСТУПА К РЕСУРСАМ КОРПОРАТИВНОЙ СЕТИ**

#### **3.1. Порядок предоставления доступа**

Доступ к ресурсам корпоративной сети предоставляется на основании заявки в АСПП.

После оформления на работу в установленном порядке на основании заявки, работнику предоставляется доступ к базовому набору ресурсов корпоративной сети.

В случае если требуется доступ к ресурсам корпоративной сети, которые не входят в базовый набор, сотрудником подается заявка в АСПП, которая в обязательном порядке согласовывается с владельцем ресурса.

#### **3.2. Порядок изменения доступа**

Изменение полномочий пользователя в рамках доступа к той или иной ИС согласовывается с руководителем заинтересованного структурного подразделения.

Основанием для предоставления доступа представителям контрагентов является договор или другой документ с обоснованием необходимости доступа и указанием списка работников, а также конкретных ИС (ресурсов), к которым необходим доступ. При этом

руководитель заинтересованного структурного подразделения обеспечивает заключение соглашения о конфиденциальности, если предполагается предоставить контрагенту доступ к сведениям конфиденциального характера.

На основании полученной и согласованной в установленном порядке заявки в АСПП администратор ИС создаёт (активирует) необходимые УЗ и назначает им соответствующие права. При назначении прав (уровня полномочий) администратор обязан руководствоваться принципом наименьших привилегий.

### **3.3. Кадровые перемещения**

При кадровых перемещениях внутри ГК, руководитель подразделения откуда увольняется сотрудник подает заявку в АСПП на блокировку прав доступа к ИТ-ресурсам компании. Руководитель подразделения куда переведен сотрудник подает заявку в АСПП на предоставление доступа с указанием информации о предыдущем месте работы (ДО, структурное подразделение, должность).

При увольнении сотрудника происходит автоматическая блокировка учетной записи с невозможностью получения доступа к ИТ-ресурсам Общества.

## **IV. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ УДАЛЕННОГО ДОСТУПА**

### **4.1. Общая информация**

Под удаленным доступом к ресурсам корпоративной сети понимаются все виды доступа, осуществляемые по внешним каналам связи. Основными видами удаленного доступа являются:

- доступ к корпоративной сети по коммутируемым каналам связи с использованием VPN каналов связи типа «точка-сеть» через сеть Интернет;
- подключение удаленных подразделений ГК к корпоративной сети с использованием VPN каналов типа «сеть-сеть» через сеть Интернет.

Удаленный доступ предоставляется:

- работникам, осуществляющим трудовую функцию на дому, находящимся в отпуске, в командировке, в деловых поездках и в иных обстоятельствах, в случае служебной необходимости;
- сотрудникам ИТ-подразделений для выполнения технологических операций по сопровождению ИТ-инфраструктуры и ИС;
- представителям контрагентов, проводящим работы в корпоративной сети.

Нарушение установленных процедур осуществления удаленного доступа к корпоративной сети и требований обеспечения его безопасности может привести к утечке

конфиденциальной информации, нанесению ущерба имиджу ГК, нарушению работоспособности информационных систем и другим негативным последствиям.

#### **4.2. Требования к организации удаленного доступа**

Удаленный доступ к ресурсам корпоративной сети предоставляется строго на основании заявки в АСПП.

Удаленный доступ пользователей к корпоративной сети может ограничиваться в зависимости от времени суток и дня недели.

Работники, которым предоставляется удаленный доступ, несут персональную ответственность за его использование только по назначению с соблюдением требований безопасности, устанавливаемых настоящей Политикой. Они обязаны принимать меры в отношении имеющихся у них компьютеров и других устройств доступа, в том числе мобильных, предназначенных для осуществления удаленного доступа к корпоративной сети, по недопущению их использования посторонними лицами.

Для организации удаленного доступа должны использоваться оборудование и/или программное обеспечение реализующие технологии IPSec и/или SSL VPN. Для VPN соединений вида «сеть-сеть» с доверенными сетями рекомендуется использовать технологию IPSec, применение которой для недоверенных сетей запрещено. Для соединений вида «точка-сеть» из любых сетей следует использовать только технологию SSL VPN. Для централизованного управления удаленным доступом рекомендуется использование сервера аутентификации.

Для снижения рисков компрометации системы защиты корпоративной сети следует использовать шлюзы для удалённого доступа, реализующие функции проверки соответствия политикам безопасности и автоматического сканирования конечных устройств перед предоставлением доступа к сети.

Общее время VPN-сессии пользователя, либо сеанса удаленного доступа не должно превышать 24 часов. По истечении этого времени сессия или сеанс должны автоматически прерываться. Для их восстановления от пользователя требуется повторное выполнение процедуры входа в сеть.

Если регистрационная запись пользователя не используется для осуществления удаленного доступа в течение 90 дней, то удаленный доступ данного пользователя к сети блокируется. Восстановление удаленного доступа в этом случае осуществляется в установленном в порядке доступа к ресурсам корпоративной сети.

## **V. ПАРОЛЬНАЯ ПОЛИТИКА**

### **5.1. Общие требования**

Пользователи корпоративной сети должны производить смену своих паролей не реже, чем раз в 90 дней. Новые пароли не должны совпадать с использовавшимися ранее. Пользователям запрещается предпринимать какие-либо действия по получению (раскрытию) паролей других пользователей.

Учетная запись пользователя блокируется после 5 неудачных попыток введения пароля (последующая разблокировка пользовательской учетной записи может производиться только сотрудниками ИТ-подразделений). Допускается настройка автоматической разблокировки учетной записи на уровне доменной политики. Включение данной настройки и ее параметров на уровне домена должно быть согласовано с начальником УИТ АО «Зарубежнефть».

Для доступа к различным информационным ресурсам и системам пользователи должны иметь строго различные пароли, не вычисляемые один из другого, а также не использовать один и тот же пароль для доступа к внутренним данным локальной сети и при использовании внешних информационных систем (например, Интернет-ресурсов).

С целью предотвращения несанкционированного доступа к рабочим местам пользователей, а также к ресурсам корпоративной сети с использованием чужих учетных записей (имен пользователей), пользователи обязаны блокировать экраны своих компьютеров в случае оставления ими своего рабочего места нажатием на компьютерной клавиатуре набора клавиш Ctrl+Alt+Del и далее – кнопки «Блокировка» («Lock Workstation») или Win + L.

### **5.2. Требования к сложности паролей**

Выбираемый пользователем пароль должен одновременно отвечать приведенным ниже требованиям:

- содержать не менее 12 символов;
- содержать цифры (0-9);
- содержать символы в верхнем и нижнем регистрах;
- содержать специальные символы (\$, #, % и т.д.);
- запрещено использовать имя своей учетной записи в пароле;
- не являться персональной информацией (имена членов семьи, адреса, телефоны, даты рождения и т.п.).

### **5.3. Ограничения**

Пользователи обязаны соблюдать необходимые меры предосторожности для обеспечения конфиденциальности своих паролей. Запрещается:

- сообщать свой пароль кому-либо, включая коллег, руководителей и специалистов ИТ-подразделений, осуществляющих техническую поддержку, по телефону, по электронной почте или какими-либо иными средствами;
- хранить пароли в доступной для чтения форме в командных файлах, сценариях автоматической регистрации, программных макросах, на компьютерах с неконтролируемым доступом, а также в иных местах, где неуполномоченные лица могут получить к ним доступ;
- записывать пароли и оставлять эти записи в местах, где к ним могут получить доступ неуполномоченные лица. Например, наклеивать листочки с записанными паролями на монитор, или складывать их в ящик стола. Допускается хранение паролей в письменном виде в личном сейфе;
- произносить свой пароль вслух в присутствии других лиц.

В случаях, когда кто-либо требует от пользователя раскрытия пароля, пользователь должен сослаться на настоящую Политику или предложить обратиться за разъяснениями к начальнику ИТ-подразделения.

Пароль должен быть немедленно изменен пользователем, если имеются основания полагать, что данный пароль стал известен кому-либо еще, кроме самого пользователя.

Сотрудникам ИТ-подразделений для выполнения своих служебных обязанностей ни при каких обстоятельствах не требуется знание паролей пользователей. Для этого у них есть все необходимые полномочия в корпоративной сети. В случае необходимости они могут произвести смену пароля пользователя, после чего должны сообщить ему об этом.

## **VI. КОНТРОЛЬ**

Общий контроль выполнения требований настоящей Политики осуществляется ИТ-подразделением. Для этого ответственным работникам ИТ-подразделения предоставляются соответствующие права доступа к ресурсам корпоративной сети (на просмотр журналов регистрации событий, таблиц доступа в ИС и т.п.).

С целью выявления попыток обхода механизмов защиты и получения несанкционированного доступа к ресурсам корпоративной сети Общества должно вестись постоянное протоколирование активности получения пользователями доступа к системам, на основе которого сотрудники ЦИБ осуществляют мониторинг этой активности.

По фактам нарушения требований настоящей Политики, повлекшим ущерб Обществу, ЦИБ в установленном порядке проводит служебные расследования, результаты которых докладываются начальнику УИТ АО «Зарубежнефть».

ЦИБ отвечает за:

- разработку политик, регламентов, инструкций, моделей угроз и прочих ВНД по вопросам обеспечения информационной безопасности;
- архитектуру систем безопасности ресурсов корпоративной сети;



- проектирование и внедрение/модернизацию средств защиты;
- мониторинг событий ИБ;
- аудит ИТ-инфраструктуры на предмет соответствия требованиям ИБ;
- разработку рекомендаций и требований по повышению защищенности ИТ-инфраструктуры;
- расследование ИБ-инцидентов;
- повышение осведомленности сотрудников ГК об актуальных киберугрозах и способах защиты.

ИТ-подразделения ДО выполняют поручения сотрудников ЦИБ и ведут операционную деятельность, связанную с предоставлением доступа к ресурсам корпоративной сети, настройкой ИТ-инфраструктуры в части требований ИБ и расследованием инцидентов.

## **VII. ОТВЕТСТВЕННОСТЬ**

Ответственность за реализацию требований настоящей Политики в части непосредственно предоставления (изменения, отмены) доступа к ресурсам корпоративной сети возлагается на ИТ-подразделение.

Работники, а также другие лица, которым предоставляется доступ к ресурсам корпоративной сети, несут ответственность за несоблюдение необходимых мер по обеспечению безопасности работы в сети в соответствии с требованиями внутренних нормативных документов.

Ответственность за обеспечение безопасности осуществления доступа к ресурсам корпоративной сети и соблюдение режима информационной безопасности лицами, не являющимися работниками ГК, при проведении ими работ в информационных системах определяется гражданско-правовыми договорами и соглашениями, заключаемыми с этими лицами.

## СПИСОК СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

### Список терминов и определений:

| Наименование термина                             | Определение термина  |
|--|--|
| <b>Администратор</b>                             | Специалист, обеспечивающий работу СИ, отвечающий за выполнение штатных технических процедур аварийного восстановления  |
| <b>Базовый набор ресурсов корпоративной сети</b> | В базовый набор ресурсов корпоративной сети входят: учетная запись в домене Active Directory; почтовый ящик; доступ к корпоративному portalу   |
| <b>Дочернее общество</b>                         | Общество, в отношении которого АО «Зарубежнефть» прямо (в силу преобладающего участия в уставном капитале) или косвенно (через третье лицо) оказывает существенное влияние на решения, принимаемые органами управления указанного общества   |
| <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>ИТ-подразделение</b>                          | УИТ в АО «Зарубежнефть» и подразделение, ответственное за информационные технологии в ДО   |
| <b>Корпоративная сеть</b>                        | Объединение информационных систем, компьютерного, телекоммуникационного и офисного оборудования всех подразделений Общества, посредством их подключения к единой компьютерной сети передачи данных с использованием различных физических и логических каналов связи  |
| <b>Пользователь</b>                              | Работник Общества, работник дочернего общества, а также прочие лица (подрядчики, аудиторы и т.п.), зарегистрированные в корпоративной сети Общества в установленном порядке и получившие права на доступ к ресурсам корпоративной сети в соответствии со своими функциональными обязанностями  |
| <b>Учетная запись пользователя</b>               | Совокупность сведений о пользователе, которая включает в себя имя пользователя и его уникальный идентификатор (далее – логин), однозначно идентифицирующий данного пользователя в операционной системе (сети, базе данных, приложении и т.п.) и служащий для определения пользовательских полномочий по доступу к ресурсам. Учётная запись создается системным администратором при |

| Наименование термина                           | Определение термина  |
|--|--|
|  | регистрации пользователя в операционной системе компьютера, в системе управления базами данных, в сетевых доменах, приложениях и т.п. Она также может содержать такие сведения о пользователе, как Ф.И.О., название подразделения, телефоны, E-mail и т.п. |
| <b>Центр информационной безопасности (ЦИБ)</b> | Отдел информационной безопасности в ООО «Нестро», централизованно обеспечивающий информационную безопасность в ГК на основе заключенных договоров  |

**Список сокращений:**

| Сокращение термина | Полное наименование термина                        |
|--------------------|--|
| <b>АСПП</b>        | Автоматизированная система поддержки пользователей |
| <b>ГК</b>          | Группа компаний АО «Зарубежнефть»                  |
| <b>ДО</b>          | Дочернее общество                                  |
| <b>ИС</b>          | Информационная система                             |
| <b>Общество</b>    | АО «Зарубежнефть»                                  |
| <b>УЗ</b>          | Учетная запись пользователя                        |
| <b>УИТ</b>         | Управление информационных технологий               |
| <b>ЦИБ</b>         | Центр информационный безопасности                  |

**Ключевые вопросы к Политике управления  
доступом к ресурсам корпоративной сети**

1. Каково назначение настоящего документа?
2. Кто имеет право получать доступ к ресурсам корпоративной сети?
3. Что представляет собой удаленный доступ к ресурсам корпоративной сети?
4. Почему удаленный доступ представляет опасность для конфиденциальных данных?
5. Какие требования предъявляются к сложности паролей?