

БҰЙРЫҚ

ПРИКАЗ

« 21 » 05 20 20 г. № 77
Нұр-Сұлтан қаласы

город Нур-Султан

**Ішкі нормативтік құжатты бекіту
туралы**

«PetroRetail» ЖШС-да (бұдан әрі – Серіктестік) парольдік қорғау туралы ішкі нормативтік құжаттың жұмыстарын ұйымдастыру және қамтамасыз етуге қойылатын талаптарға байланысты **БҰЙЫРАМЫН:**

1. «PetroRetail» ЖШС-да, оның филиалдары мен еншілес ұйымдарында парольдік қорғау ережесі туралы қоса берілген ішкі нормативтік құжаты (бұдан әрі – ІНҚ) бекітілсін.
2. Құрылымдық бөлімшелердің басшылары мен Серіктестік филиалдарының директорлары қызметкерлерді ІНҚ-мен таныстыруды ұйымдастырсын.
3. ІНҚ орындауға жауапкершілік ақпараттық технологиялар департаментінің директорына жүктелсін.
4. Осы бұйрықтың орындалуын бақылауды өзіме қалдырамын.

Бас директор

Т. Шотанов



Орынд. Т.Байбусинов
ІР - 1158

БҰЙРЫҚ

ПРИКАЗ

« 21 » 05 20 20 г.№ 77
Нұр-Сұлтан қаласы

город Нур-Султан

**Об утверждении внутреннего
нормативного документа**

В целях требований к организации и обеспечению работ внутреннего нормативного документа о парольной защите в ТОО «PetroRetail» (далее – Товарищество), **ПРИКАЗЫВАЮ:**


1. Утвердить прилагаемый внутренний нормативный документ о правилах парольной защиты в ТОО «PetroRetail», его филиалах и дочерних организациях (далее – ВНД).
2. Руководителям структурных подразделений и директорам филиалов Товарищества организовать ознакомление работников с ВНД.
3. Ответственность за исполнение ВНД возложить на директора департамента информационных технологий.
4. Контроль за исполнением настоящего приказа оставляю за собой.

Генеральный директор

Т. Шотанов



Исп. Т.Байбусинов
IP - 1158

 PETRO RETAIL	Внутренний нормативный документ о парольной защите в ТОО «PetroRetail»	
Редакция 1	Стр.1 из 7	Утвержден приказом генерального директора от « <u>21</u> » <u>05</u> 2020 г. № <u>77</u>

1. Цель документа

1. Настоящий внутренний нормативный документ о парольной защите (далее ВНД) разработаны для Товарищества с ограниченной ответственностью «PetroRetail» а также его филиалов и дочерних организаций (далее - Товарищество) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления/блокировка учетных записей пользователей) используемых в информационном пространстве (далее - ИП) меры обеспечения безопасности при использовании паролей, а также контроль за действиями пользователей и обслуживающего персонала ИП при работе с паролями.

2. Настоящее ВНД призвано решать три основные задачи:

- защита ценной информации от ознакомления с ней посторонних лиц;
- учет доступа к сведениям конфиденциального характера: персональным данным, коммерческой тайне;
- обеспечение личной ответственности работников за свои действия.

3. Требования настоящего ВНД являются неотъемлемой частью комплекса мер безопасности и защиты информации в Товариществе, распространяются на всех работников Товарищества, использующих в работе средства вычислительной техники, программное обеспечение (далее - ПО) и информационные системы (далее - ИС) и применительны для всего ИП Товарищества.

4. В ВНД предоставлен набор правил работы с паролями, которые включают в себя такие важные условия, как требования к сложности пароля, к длине пароля, к частоте смены пароля, критерии, по которым можно судить о недопустимости пароля, способы хранения и замены паролей. Все пароли пользователей, а также системных учетных записей должны соответствовать данному внутреннему нормативному документу.

2. Область применения

- 2.1. Основу функционирования механизмов распределения логического доступа к ИС и данным составляют принципы идентификации и аутентификации.
- 2.2. В значительной части систем в качестве фактора аутентификации используется знание субъектом (Пользователем) и только им секретной последовательности символов – пароля либо цифровой последовательности для доступа.

Разработал: Байбусинов Т.Е. 	Проверил: Даулеткалиев А.Е. 
---	---

- 2.3 Необходимость обеспечения адекватной защиты в соответствии с требованиями, выдвигаемыми Товариществом к ИБ, относится ко всем задачам и процессам.
- 2.4. Защита данных, основанная на разграничении доступа по предъявлению пароля, является одним из элементов безопасности Товарищества и входит в механизмы управления доступом к большинству ИС Товарищества.

3. Определения и сокращения

Товарищество с ограниченной ответственностью	ТОО «PetroRetail»
Аутентификация	Процедура проверки соответствия предъявленного идентификатора субъекту или объекту ИС;
Пароль	Условное слово или набор знаков, предназначенный для подтверждения личности или полномочий, чаще всего пароли используются для защиты информации от несанкционированного доступа;
ПИН	Персональный идентификационный номер, числовая последовательность, на основе которой предоставляется право на доступ к информации на защищенном внешнем носителе;
Пользователи	Работники Товарищества и третьи лица, имеющие доступ к информационным ресурсам Товарищества;
Информационная безопасность	Процесс обеспечения конфиденциальности, целостности и доступности информационного пространства Товарищества, который определяется отсутствием недопустимых рисков, связанных с утечкой информации по техническим каналам, с несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы информационных систем, с поломкой компонентов IT-инфраструктуры, которые могут вызвать перерывы в работе;
Администратор	Структурное подразделение, являющееся заказчиком ИС, которые позволяют автоматизировать ряд обязанностей структурного подразделения, производящие настройку соответствующих механизмов безопасности;

Информационная система (ИС)	Система, предназначенная для автоматизации целенаправленной деятельности конечных Пользователей, обеспечивающая, в соответствии с заложенной в нее логикой обработки, возможность получения, модификации и хранения информации;
Средства автоматизации	Автоматизированное рабочее место, включающее периферийные устройства для функциональной деятельности работника Товарищества, а также организационная техника. К средствам автоматизации подлежат мониторы, системные блоки, принтеры, ксероксы, сканеры, IP-телефоны и т.д;
ActiveDirectory	Реализация службы каталогов корпорации Microsoft для операционных систем семейства Windows Server английского языка «Активный каталог»);
Конфиденциальность	Свойство, указывающее, что информация остается недоступной или нераскрытой для неавторизованных физических и юридических лиц или процессов;
Информационное пространство Товарищества (ИП) –	Пространство Товарищества, состоящее из информационных, технических ресурсов и систем, целенаправленно обеспечивающих, коммерческую, административную и организационную деятельности, а также взаимодействие участников данного ИП;
Администратор КВС	Сотрудник, ответственный за работу корпоративной сети или её части, обеспечивающий и контролирующий качество физической связи КВС, настройку активного оборудования, настройку общего доступа и предопределённого круга программ, обеспечивающих стабильную работу сети;
ИР	Информационные ресурсы.
ДИТ	Департамент информационных технологий

4. Ответственность

4.1. В случае передачи пароля пользователя третьим лицам ответственность за разглашение полученного пароля и действия, произведенные на персональном компьютере, возлагается на администратора ИР/КВС и на лицо, получившее пароль.

4.2. За утерю, передачу паролей, повлекших за собой разглашение конфиденциальной информации пользователь ИР/КВС привлекается к ответственности в соответствии с утвержденными ВНД Товарищества и с действующим законодательством РК.

4.3. Выявленное нарушение требования настоящего ВНД подлежит служебному расследованию.

4.4. Сотрудник, ответственный за информационные технологии Товарищества несет ответственность за ознакомление работников, использующих ПО, ИС, средства вычислительной техники, с требованиями ВНД под роспись, с обязательным уведомлением работника о персональной ответственности за использование паролей, не соответствующих предъявленным требованиям, а также за разглашение парольной информации.

4.5. Работник сектора автоматизации филиала несет ответственность за восстановление пароля без уведомления службы технической поддержки.

4.6. Подразделение ДИТ проводит выборочный контроль выполнения сотрудников Товарищества требований ВНД.

4.7. Ответственность за неисполнение и/или ненадлежащее исполнение требований настоящих ВНД возлагается на виновных лиц в порядке, установленном законодательством Республики Казахстан, а также утвержденных ВНД Товарищества.

4.9. При выявлении нарушения требований настоящих ВНД проводится служебное расследование в установленном в Товариществе порядке.

4.10 Все работники, обеспечивающие выполнение настоящих ВНД, должны быть ознакомлены под роспись с требованиями настоящих ВНД.

5.Способ осуществления ВНД

- 5.1. Все Пользователи, имеющие собственный пароль или ПИН, сохраняют его в тайне, запоминают его либо фиксируют недоступным для посторонних лиц способом. Товарищество не предусматривает никаких случаев, создающих условия для передачи пароля или ПИНа от одного сотрудника другому.
- 5.2. При проведении классификации данных ИС, пароли (как данные) должны быть отнесены к наиболее высокому разделу классификации для указанной системы.
- 5.3. Механизм парольной защиты ИС должен обеспечивать сохранение пользовательских паролей в зашифрованном виде, препятствующем их несанкционированному извлечению.
- 5.4. Если в рамках работы ИС возникает необходимость пересылки пароля, ПИНа или связанных данных между средствами автоматизацией или вне ее, пересылаемые данные должны быть надежно защищены и скрыты.
- 5.5. Если Пользователь работает в нескольких ИС, не объединенных одним паролем он использует различные пароли для входа в разные системы.

- 5.6. Администраторы ИС должны хранить пароли ИС в специально отведенном хранилище (сейфе), препятствующем их несанкционированному извлечению.
- 5.7. Если ИС предполагает наличие при своей установке специальных учетных записей, то перед вводом ИС в эксплуатацию, указанные учетные записи должны быть заблокированы либо пароли к ним должны быть заменены.
- 5.8. Товарищество не допускает использование в ИС групповых идентификаторов и паролей.
- 5.9. Парольная защита, используемая в ИС должна иметь минимальные требования возможности установки следующих ограничений, пароль должен состоять не менее чем из восьми и более символов;
- 1) содержит сочетание букв верхнего и нижнего регистров (например, a-z, A-Z);
 - 2) включает цифры;
 - 3) не является часто употребляемым словом на любом языке, диалекте, сленге и т.д.;
 - 4) не основан на персональной информации, к примеру фамилии, дате рождения и т.д.;
 - 5) не содержат компьютерные термины и названия, команды, названия сайтов, компаний, оборудования, программного обеспечения;
 - 6) не содержат название вашей компании и географические наименования, к примеру: "Алматы" или их производные;
 - 7) перечисленные примеры с цифрой в начале или конце пароля;
 - 8) номера телефонов или группы символов, состоящие из одних цифр;
 - 9) срок использования персональных паролей не должен превышать 60 дней (для рабочих станции и АСУ на АЗС – 90 дней);
 - 10) срок использования системных/интеграционных паролей не должен превышать 180 дней;
 - 11) история паролей (запрет на использование предыдущих паролей) должна быть не менее четырех вариантов;
 - 12) при вводе пароля Пользователем, вводимые символы не должны отображаться на экране либо должны маскироваться другими символами;
- При технической возможности информационной системы:
- 13) Время до сброса счетчика блокировки – 20 минут;
 - 14) Пороговое значение блокировки – 5 ошибок входа в систему;
 - 15) Продолжительность блокировки учетной записи – 20 минут;
- 5.10. Пользователь не должен просить или принимать помощь в формировании своего пароля от постороннего, в том числе от любого работника Товарищества.
- 5.11. Ввод пароля в ИС Пользователь осуществляет таким образом, чтобы находящиеся рядом люди или наблюдающие объекты не могли произвести визуальное отслеживание последовательности ввода.

- 5.12. Администратор должен установить параметр смены временного пароля при первом входе для нового Пользователя любой ИС (если данный параметр присутствует в ИС).
- 5.13. Пользователь после получения доступа к функции изменения пароля может изменить временный пароль на свой собственный пароль.
- 5.14. СТРОГО запрещается:
- где-либо записывать пароль;
 - передавать любые свои персональные авторизационные учетные данные (логин и пароль) третьим лицам;
 - передавать пароли пользователям при помощи почтовых сообщений, по телефону, по электронной почте, либо иным другим открытым способом;
 - упоминать о содержимом пароля (например, "мой день рождения");
 - указывать свой пароль в анкетах или опросниках;
 - хранить пароль в файле на компьютере, включая переносной, без шифрования;
 - использовать функцию "Запомнить пароль" в таких приложениях как браузеры, мессенджеры, почтовые программы;
 - создание и использование локальных учетных записей на рабочих станциях, подключенных к КВС Товарищества и входящих в состав домена, либо в состав какого-либо из его поддоменов.
- 5.15. Во время ввода паролей, необходимо исключить возможность распознавания его посторонними лицами или компрометации пароля посредством технических средств. Ввод пароля осуществляется с учётом регистра (верхний-нижний) и с учётом текущей раскладки клавиатуры (EN-RU и др.).
- 5.16. Компьютер не допускается оставлять без контроля. При временном оставлении рабочего места в течение рабочего дня рабочая станция в обязательном порядке блокируется нажатием комбинации клавиш «Win + L» или настроить автоматическое включение экранной заставки, защищенной паролем.
- 5.17. Для защиты пароля при технической возможности администратору ИР/КВС необходимо настроить механизм блокировки при введении определенного количества неверных вариантов пароля. Количество ввода неверных паролей пользователей определяется отдельно для каждого ИР/КВС и прописывается в правовых и регламентирующих данный ресурс, документах. В случае неудавшейся попытки авторизации в журнале учета работ ИР/КВС должно заноситься соответствующее сообщение. При многократных неудавшихся попытках авторизации должно генерироваться предупреждение системы обнаружения вторжений.
- 5.18. При приеме на работу вновь принятому (далее - новому) сотруднику, администратор ответственный за функционирование ИР/КВС должен осуществить передачу временного пароля, непосредственно новому

- сотруднику. После получения, сотруднику необходимо зайти в систему и заменить пароль.
- 5.19. В случае интеграции информационного ресурса с Active Directory используется учетная запись и пароль, выдаваемые для работы с КВС.
- 5.20. При приеме на работу администратора ИС, администратора КВС, системного администратора руководитель соответствующего подразделения, должен ознакомить нового сотрудника с документацией, связанной с информационной безопасностью и выдать учетные данные (логин и пароль) согласно правилам, утвержденным в правовых и регламентирующих данный ресурс, документах.
- 5.21. С лицами, работающими на правах аутсорсинга (далее - Контрагент), необходимо заключение контракта, в котором определяются права на предоставление доступа к информационным ресурсам Товарищества. Как и в случае с приемом нового сотрудника Контрагенту выдается учетная запись с паролем, которая должна быть заблокирована/удалена Администратором ИР/КВС в течении 3-х рабочих дней после подписания акта выполненных работ.
- 5.22. При наступлении момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника) учетная запись должна немедленно блокироваться, используя механизмы автоматического блокирования учетных записей уволенных сотрудников, используя соответствующие ИС. При невозможности автоматического блокирования учетных записей, руководитель структурного подразделения обязан своевременно посредством СЭД подать заявку в ДИТ на блокирование учетной записи сотрудника в соответствующих ИС не позднее, чем за сутки до момента прекращения срока действия полномочий пользователя (окончание договорных отношений, увольнение сотрудника, выход в трудовой отпуск, временная нетрудоспособность, отпуск по уходу за ребенком и т.д).
- 5.23. В случае утери или компрометации (разглашения, утраты) или подозрения в компрометации пароля пользователя, пользователь обязан немедленно направить заявку в службу технической поддержки по электронной почте techsupport@petroretail.kz. В выходные и праздничные дни электронная почта будет предоставлена после заключения договора на техническое обслуживание.
- 5.24. Внесение изменений в настоящее ВНД может производиться по результатам анализа инцидентов ИБ, актуальности, достаточности и эффективности используемых мер обеспечения ИБ, результатам проведения внутренних аудитов ИБ и других контрольных мероприятий.