П Р И К А З

«____»_____2018 г. г. Москва №_____

О парольной защите в ООО «Сатурн»

В целях повышения уровня обеспечения информационной безопасности, информационно-телекоммуникационной инфраструктуры (ИТКИ) Компании,

П Р И К А З Ы В А Ю :

1. Утвердить инструкцию парольной защиты информационных ресурсов ООО «Сатурн» (Приложение №1).
2. Заместителям генерального директора, руководителям функциональных блоков и структурных подразделений организовать изучение Инструкции, указанной в п.1 настоящего приказа, с работниками, и обеспечить выполнение изложенных в ней требований при выполнении своих должностных обязанностей.
3. Директору департамента информационных технологий …:

3.1. Привести парольную политику ООО «Сатурн» в соответствии с пунктом 2 Инструкции, указанной в п.1 настоящего приказа.

Срок: 5 рабочих дней с даты выхода настоящего приказа

3.2. Провести внеплановую смену администраторских и пользовательских паролей.

Срок: 10 рабочих дней с даты выхода настоящего приказа.

4. Контроль исполнения настоящего приказа возложить на ….

Генеральный директор …

Приложение №1
к приказу ООО «Сатурн»
от «__» _____ 2018 г.
№ _____

ИНСТРУКЦИЯ
парольной защиты информационных ресурсов ООО «Сатурн»

1. Аннотация

Настоящая Инструкция разработана для использования работниками структурных подразделений ООО «Сатурн» (далее - Компания) с целью усиления парольной защиты информационно-телекоммуникационной инфраструктуры, в информационных системах персональных данных (далее – ИСПДн) Компании, минимизации рисков несанкционированного доступа и снижению финансовых рисков, связанных с парольной политикой.

Целевой пользователь документа – работники Общества.

2. Требования

Все правила в области парольной политики, применяемые в Компании, в случае их регламентации, при генерации (создании) новых парольных фраз должны быть оптимизированы с учетом следующих требований:

– Парольные фразы системных учетных записей (администратора домена, локального администратора, пользователя и т.д.) должны изменяться ежеквартально.

– Запрещается передача парольных фраз пользователям при помощи почтовых сообщений либо иным открытым способом через Интернет. Открытый способ – такой способ передачи, при котором информация, попавшая к третьему лицу, может быть прочитана без использования парольной или криптографической информации.

– Запрещается записывать свой пароль на бумаге, в файле, мобильных средствах и других носителях информации, в том числе на предметах. А также хранение его на рабочем месте.

– Запрещается использовать для хранения хэша паролей алгоритм Microsoft LAN Manager (LM).

– Парольная фраза учетной записи пользователя, имеющего административные привилегии, полученные при помощи членства в группе или при помощи программ, должна быть отличима от других парольных фраз учетных записей данного пользователя.

– При смене пароля новое значение должно отличаться от предыдущего не менее чем в 3 позициях символов.

– Все парольные фразы пользователей, а также системные парольные фразы должны соответствовать правилам сложности образования (создания, генерации) паролей. Правила сложности образования паролей включает следующие положения:

– При образовании парольных фраз следует учитывать, что:

– Парольные фразы должны содержать не меньше одного спецсимвола (!@#$%^&*()_+|~-=\`{}[]:";'<>?,./), буквы в различном регистре и цифры.

– Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т.д.), последовательности символов и знаков (111, qwerty, abcd и т.д.), общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно угадать, основываясь на информации о пользователе.

– Недопустимо хранение парольных фраз в доступном для любых третьих лиц виде.

– Длина парольной фразы должна составлять не менее 8 символов.

3. Требования к передаче парольно-ключевой информации

В случае незапланированного отсутствия работника на рабочем месте передача парольно-ключевой информации возможна в случае служебной (оперативной) необходимости. Работник имеет право передать свои учетные данные от автоматизированной рабочей станции, электронной почты, от ИСПДн («…», «…», «…») (за исключением ограничений, установленных законодательством Российской Федерации в области защиты информации и коммерческой тайны) непосредственному руководителю (или лицу его замещающему) для решения оперативных задач в целях поддержания непрерывности рабочего процесса. Передача парольной информации должна осуществляться способом, отвечающим требованиям конфиденциальности, с учетом фактической ситуации внепланового отсутствия. По возвращению к должностным обязанностям работник обязан изменить пароль своей учетной записи. Ответственность за полученную парольно-ключевую информацию и ресурсы ею защищаемые возлагается на лицо, получившее такой доступ.

В непредусмотренных настоящими требованиями случаях (например, невозможности установления связи с работником) допускается следующий механизм получения парольно-ключевой информации: работник, которому необходимо получить доступ к автоматизированному рабочему месту, почтовому ящику, ИСПДн по согласованию с руководителем структурного подразделения (или лицом его замещающим) обращается в Департамент по безопасности в рабочем порядке. Работник Департамента по безопасности, установив возможность предоставления доступа, совместно с работником ДИТ предоставляет доступ к автоматизированному рабочему месту посредством использования учетной записи Администратора.

Передача парольно-ключевой информации (логина и/или пароля) третьим лицам запрещена.

4. Рекомендации

В целях усиления уровня защищенности при применении правил парольной защиты пользователям следует придерживаться следующих рекомендаций:

– При вводе пароля, пользователю необходимо исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерами и т.п.).

– В случае прекращения полномочий пользователя (увольнение, либо переход на другую должность) производится немедленное удаление пароля сразу после окончания его последнего дня работы.

– Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение или переход на другую работу) администраторов информационной системы и других работников, которым по функциональным обязанностям были предоставлены полномочия по управлению системой парольной защиты.

– Не используйте один и тот же пароль для доступа к учётным записям Общества и к другим ресурсам (например, доступ в интернет из дома, системам электронной коммерции и т. д.). По возможности не используйте один и тот же пароль для доступа к различным ресурсам внутри Общества. Например, используйте один пароль для прикладных программ и другой для администрирования ресурсов. Используйте различные пароли для учётных записей различных систем.

– Не использовать ранее использованные пароли.

– Не сообщайте никому свой пароль по телефону.

– Не отправляйте свой пароль по электронной почте.

– Не говорите о своём пароле рядом с посторонними.

– Не упоминайте о содержимом пароля (например, «мой день рождения»).

– Не указывайте свой пароль в анкетах или опросниках.

– Не храните пароль в файле на компьютере, включая переносной, без шифрования.

– Не используйте функцию «Запомнить пароль», например, в таких приложениях как Internet Explorer, FireFox, Google Chrome и т.д.

– Если кто-либо требует сообщить ваш пароль, сошлитесь на этот документ или попросите позвонить в Департамент по безопасности.

– Если вы считаете, что учётная запись или пароль скомпрометированы, сообщите об этом в Департамент по безопасности и смените все пароли.

5. Ответственность

Работники Общества несут ответственность за сохранность парольной информации и соблюдение положений настоящей инструкции. В случае выявления нарушений, к нарушителям могут быть применены меры дисциплинарного взыскания в соответствии с действующим законодательством Российской Федерации.

Владельцы личных паролей должны быть ознакомлены под подпись с данной инструкцией и предупреждены об ответственности за разглашение парольной информации.

Департамент по безопасности совместно с Департаментом информационных технологий организуют периодический контроль на рабочих местах пользователей за правильностью обращения с личными паролями, соблюдением порядка их смены и хранения. В случае выявления нарушений установленного порядка работы с личными паролями или нарушения функционирования автоматизированного рабочего места пользователя требовать прекращения обработки информации, как для отдельных пользователей, так и в подсистеме в целом до выяснения их причин и замены личного пароля пользователя (пользователей).