Приложение
к Приказу АО «Казахтелеком»
от «__» _____ 2023 года
№ _____

Политика парольной защиты АО "Казахтелеком"

Алматы, 2023г.

Оглавление

1 Термины, сокращения и определения

Администратор ИС – привилегированный пользователь, имеющий расширенные полномочия (привилегии) по настройке и эксплуатации ИС, а так же по управлению доступом к ИС;
ИБ – информационная безопасность. Состояние защищённости информационных ресурсов и систем, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность, что достигается комплексом организационных и технических мер, направленных на защиту данных;
ИР – информационный ресурс (актив). В рамках настоящей Политики понимается упорядоченная совокупность информации, представленная в электронном виде (файлы, базы данных, алгоритмы, компьютерные программы, приложения и т.д.) и содержащаяся, хранящаяся, обрабатываемая, передаваемая и используемая в ИС Общества (сети передачи данных, системы хранения, обработки, передачи, визуализации информации и т.п.);
ИС – информационная система. Система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением соответствующих организационных ресурсов (человеческих, технических, финансовых и т. д.);
ИТ – информационные технологии. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;
НРД – нормативно-регламентирующая документация Общества (политики, стандарты, приказы, регламенты, руководства, инструкции и т.п.);
НСД – несанкционированный доступ. Доступ к информации или ресурсам ИС, осуществляемый с нарушениями установленных правил и/или правил доступа;
Общество – АО «Казахтелеком»;
ПО – программное обеспечение;
Политика – утвержденная в Обществе настоящая Политика парольной защиты АО "Казахтелеком;
Пользователь – работник Общества или представитель третьей стороны, работающий с ИС Общества и использующий её ИР в соответствии с установленными правами и правилами доступа к информации;
СВТ – средства вычислительной техники (стационарные компьютеры или рабочие станции, переносные компьютеры или ноутбуки и т.п.);
СП – структурное подразделение Общества;
СП ТП – структурное подразделение Общества либо подразделение (или организация), привлекаемое для выполнения данных функций, которое выполняет техническую поддержку пользователей и СВТ в Обществе;
Третья сторона, третье лицо – физическое или юридическое лицо, подрядчик, поставщик, партнер, контрагент, контрактник, и т.п., взаимодействующие с Обществом на основании договорных соглашений и не являющееся штатным работником Общества;
KeePass - кроссплатформенная свободная программа для хранения паролей;
SNMP (англ. Simple Network Management Protocol) – простой протокол сетевого управления;

sudo (англ. substitute user and do, дословно «подменить пользователя и выполнить») – программа для системного администрирования UNIX-систем, позволяющая делегировать те или иные привилегированные ресурсы пользователям с ведением протокола работы.

2 Назначение Политики и область ее действия

1. Политика регламентирует организационно-техническое обеспечение процессов создания, использования, смены, прекращения действия паролей учетных записей пользователей и администраторов ИС Общества, а также контроля действий при работе с паролями.
2. Политика является регламентирующим документом и предназначена для обязательного использования в Обществе.
3. Пароли являются важнейшим аспектом ИБ, первичным методом защиты доступа к ИС Общества, обеспечивают разграничение прав пользователей и защиту учетных записей пользователей. Неправильно выбранный пароль повышает потенциальный риск НСД к ИС Общества.
4. Выполнение этой Политики минимизирует вероятность нарушения режима ИБ Общества при злоупотреблениях с паролями.
5. Все работники Общества и представители третьих сторон, имеющие доступ к ресурсам ИС Общества, ответственны за правильный выбор и хранение паролей в соответствии с требованиями Политики и несут ответственность за невыполнение этих требований.
6. Действие Политики распространяется на всех, кто имеет доступ или ответственен за предоставление доступа к любой ИС Общества, включая все площадки, и все компоненты ИТ-инфраструктуры Общества.
7. Политика предназначена для распространения внутри Общества и предоставления всем Руководителям, Работникам Общества и прочим заинтересованным лицам – участникам бизнес-процессов Общества.

3 Общие положения и требования политики

8. Политика разработана в соответствии с законодательством Республики Казахстан в сфере ИБ, НРД регулятора (регулирующих и надзорных органов), Политикой ИБ Общества, Концепцией ИБ Общества, международными стандартами по ИБ ISO/IEC 27000, COBIT, ITIL, современным состоянием и ближайшими перспективами развития информационной структуры Общества, возможностей современных организационно-технических методов защиты информации.
9. Пересмотр положений Политики осуществляется на постоянной основе, но не реже одного раза в два года.
10. Внеплановый пересмотр Политики осуществляется в случае:

1) изменения нормативно-правовых документов Республики Казахстан, НРД регулятора (регулирующих и надзорных органов), внутренних документов Общества, определяющих требования ИБ;

2) выявления снижения общего и/или частного уровня ИБ Общества (по результатам внутреннего или внешнего аудита);

3) существенных изменений организационной и/или инфраструктуры, ресурсов и бизнес-процессов Общества;

4) выявления существенных недостатков или противоречий положений Политики с другими внутренними документами Общества.

11. Положения Политики, могут дополняться, но не отменяться (заменяться), положениями других частных политик ИБ Общества и документами, разработанными на их основе.

12. Дополнительную информацию о безопасной работе и защите информации в ИС Общества можно получить из других частных политик ИБ Общества.

13. В основе Политики лежит структурный подход к парольной защите, при котором должны обеспечиваться следующие условия:

1) пароль является средством защиты информации, СВТ, ПО, серверов, приложений, активного оборудования передачи данных и сведений конфиденциального характера от НСД и представляет собой числовую и символьную последовательность, состоящую из определенного количества знаков и символов;

2) пароль должен держаться в тайне и эффективен как средство защиты только при правильном его использовании;

3) пароли должны храниться в электронном виде только в защищенной форме.

14. Идентификатор и пароль пользователя в ИС являются учётными записями (данными), на основании которых пользователю предоставляются права доступа к техническим средствам и ИС, протоколируются производимые им в ИС действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) пользователем информации.

15. Пользователь обязан помнить свои идентификатор и пароль.

16. Пароли могут быть личными (персональными, индивидуальными) и групповыми (общими, коллективными).

17. Личный пароль должен принадлежать только одному пользователю и применяться для разграничения доступа в многопользовательских ИС, а также доступа к ресурсам индивидуального пользования.

18. Личные пароли доступа к ресурсам ИС должны устанавливаться первый раз, как правило, администраторами ИС. После первого входа в ИС и в дальнейшем пароли должны выбираться, создаваться и использоваться пользователями ИС самостоятельно с учетом требований Политики.

19. Групповой пароль должен принадлежать нескольким пользователям, которые объединяются в соответствующую группу по каким-либо признакам и правилам, и применяется в многопользовательских ИС для доступа к общим ресурсам и/или в ИС с одним технически возможным паролем, если требуется обеспечить доступ к ИС нескольких пользователей.

20. Процессы создания и использования групповых паролей должны согласовываться и строго контролироваться СП ИБ. Создание групповых паролей в ИС должно выполняться администраторами ИС с соответствующими привилегиями и с соблюдением требований положений Политики.

21. Пароль учетной записи пользователя, имеющего административные привилегии, полученные различным путем, например, при помощи членства в группе или при помощи программ, например, таких как sudo, должен быть уникален по отношению к другим паролям учетных записей данного пользователя.

22. Все пароли административных (системных) учетных записей, а также пароли приложений и активного оборудования необходимо хранить в базе данных в зашифрованном виде, доступ к которой ограничен.

23. Запрещается:

1) сообщать свой пароль кому-либо;

2) использовать одну и ту же персональную учетную запись разными пользователями;

3) использовать один и тот же пароль для доступа к различным ИС;

4) использовать тот же самый пароль, что и для других систем (например, домашний Интернет, бесплатная электронная почта, форумы и т.п.);

5) передача паролей с использованием третьих лиц, незашифрованной электронной почты либо иным другим открытым способом через Интернет;

6) хранение паролей в открытом виде на любых видах носителей информации, в том числе записанных на бумаге и в легко доступном месте;

7) в открытом виде содержание паролей в текстах программ или файлах и их запись на любые виды носителей информации.

24. Передачу паролей разрешается осуществлять в следующих случаях:

1) Передача пароля от работника руководителю СП при возникновении производственной необходимости в случае временного отсутствия работника;

2) передача паролей от работника руководителю СП в случае прекращения его полномочий (увольнение и т.п.) и невозможности аннулирования учётной записи с обязательной последующей сменой пароля;

3) передача паролей между работниками в случае использования групповых учетных записей или общих адресов рабочей электронной почты для исполнения должностных обязанностей;

4) передача паролей для хранения руководителю СП подразделения в соответствии с пунктом 25 Политики.

25. Хранение паролей на бумажном носителе допускается только в личном сейфе (или в личном опечатываемом, запирающемся шкафу) или в сейфе (или в опечатываемом, запирающемся шкафу) руководителя СП в закрытом конверте. При возникновении производственной необходимости в случае временного отсутствия работника или в случае прекращения его полномочий (увольнение и т.п.) руководителю СП разрешается вскрыть конверт с паролем.

26. Допустимо хранение паролей пользователей на СВТ Общества в файлах, не доступных другим пользователям (т.е. исключительно на локальных дисках, не на сетевых и не в общих папках). В таких случаях необходимо хранить пароли в зашифрованном виде (например, с помощью программы KeePass, зашифрованного архива и т.п.).

27. Пароли администраторов ИС (системных, сетевых администраторов, администраторов прикладных систем, администраторов информационной безопасности и т.д.) должны храниться в соответствии с пунктом 25 Политики. Сразу же после смены паролей их новые значения (вместе с именами соответствующих учетных записей) администратор ИС обязан в запечатанном конверте передать на хранение руководителю СП.

28. В случае необходимости (внештатные ситуации, форс-мажорные обстоятельства и т.п.) использования пароля администратора ИС в его отсутствие

конверт с паролем выдается руководителем СП работнику, производящему работы с ИС, под роспись. В таком случае, отсутствовавший ранее администратор ИС должен сменить свой пароль немедленно после возвращения на рабочее место.

29. В случае, если кто-либо требует от пользователя сообщить его пароль, то пользователю необходимо сослаться на настоящую Политику, уведомить непосредственного руководителя и/или направить требующего в СП ИБ для получения разъяснений по данному вопросу.

30. Пользователь должен принять все меры для того, чтобы исключить возможность компрометации принадлежащего ему пароля.

31. Пользователь несет персональную ответственность за сохранность своего пароля в конфиденциальности.

32. О любых фактах компрометации необходимо информировать непосредственного руководителя СП и СП ИБ любым доступным и принятым в Обществе способом.

33. При создании новой учетной записи в соответствующей ИС и/или выполнении процедур по ее замене, восстановлению, разблокированию и т.п., требуется средствами самой ИС и/или силами администратора ИС сгенерировать и присвоить пользовательской учетной записи временный пароль. Последующие действия описаны в п.18 данной Политики.

34. Временные пароли должны назначаться пользователю только после его идентификации.

35. Временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю.

36. При использовании SNMP-протокола, необходимо использовать отличные от стандартных значений строк подключений (Community Name) «public», «private», «system» и отличными от пароля, используемого для входа в систему.

37. Со стороны СП ИБ в рамках проведения аудитов ИБ должны выполняться мероприятия по проверке различных паролей на стойкость к взлому и подбору. Если во время таких мероприятий пароль будет подобран или взломан, то соответствующая учетная запись должна блокироваться, а пользователь и администратор ИС должны получить соответствующее уведомление (замечание) и указания для выполнения процедур по смене пароля и разблокирования учетной записи.

38. Все пароли пользователей, администраторов, а также системные пароли должны соответствовать требованиям Политики.

4 Правила формирования пароля

39. Формирование паролей производится в соответствии с требованиями положений Политики в рамках выполнения различных процедур (методик, регламентов, инструкций, правил и т.п.) по обслуживанию (эксплуатации, администрированию, операционному управлению и т.п.) ИС Общества.

40. При создании любого пароля следует руководствоваться следующими требованиями:

1) длина пароля для пользователей должна быть не менее восьми символов;

2) длина пароля для административных (системных) учетных записей должна быть не менее десяти символов;

3) пароль должен содержать буквы в нижнем и верхнем регистрах (строчные и ПРОПИСНЫЕ), десятичные цифры и/или специальные символы (@ # $ & * % и т.п.);

4) пароль не должен содержать имя учетной записи пользователя или какую-либо его часть или включать в себя легко вычисляемые сочетания (номера телефонов, имена, фамилии, даты дней рождения, наименования СВТ и т.д.), а также общепринятые сокращения (LAN, USER и т.п.).

41. При формировании паролей, по возможности, должны использоваться специальные средства контроля, не позволяющие пользователям выбирать плохие и «слабые» пароли, т.е. такие пароли, которые не соответствуют требованиям Политики.

42. Для генерации паролей допустимо использовать любую систему или ПО, удовлетворяющие требованиям Политики.

43. Администраторы ИС, в обязанности которых входит создание и удаление учетных записей пользователей, не должны иметь доступ к значениям личных паролей пользователей.

5 Правила ввода пароля

44. Ввод пароля осуществляется согласно следующих правил:

1) ввод пароля должен осуществляться непосредственно пользователем ИС (владельцем пароля);

2) при вводе пароля символы не должны отображаться на экране в явном виде;

3) в целях предотвращения неверного ввода пароля пользователь должен убедиться в правильности выбранного языка ввода (раскладки клавиатуры), а также исключить возможность просмотра, набираемого на клавиатуре посторонними лицами;

4) ИС должны настраиваться таким образом, чтобы после 5 неудачных попыток ввода пароля учётная запись блокировалась на 10 минут. При систематической блокировке учётной записи пользователя (более 3 раз подряд), что может свидетельствовать о возможной атаке, взломе или иных нарушениях ИБ, учетная запись должна блокироваться на постоянно;

5) возобновление заблокированной учетной записи пользователя должно осуществляться на основании зарегистрированного обращения пользователя в СП ТП, после получения согласования от СП ИБ;

6) при плановой или внеплановой смене пароля необходимо произвести ввод нового пароля два раза.

6 Порядок смены пароля

45. Любые пароли должны периодически меняться. При отсутствии иных НРД Общества, регламентирующих периодичность смены пароля в конкретном случае и для конкретной ИС, пароль должен меняться в соответствии с требованиями положений Политики.

46. Плановая смена паролей производится не реже одного раза в 3 месяца для пользовательских учетных записей и не реже одного раза в 6 месяцев для административных (системных) учетных записей (администратор домена, локальный администратора, root и т.д.).

47. При смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;

48. Уникальность паролей должна быть обеспечена в течение 9 периодов их действия.

49. Целевая ИС, к которой подключается пользователь с временным паролем, по возможности, должна быть настроена таким образом, чтобы требовать от пользователя выполнения смены временного пароля и предоставлять ему эту возможность. В случае отсутствии данной функциональности в ИС, должны обеспечиваться условия и предоставляться соответствующие права, позволяющие выполнять процедуру по смене временного пароля пользователем самостоятельно.

50. В случае прекращения полномочий (увольнение и т.п.) работника, который имел доступ к сервисным, системным или групповым учетным записям, должна производиться смена паролей данных учетных записей.

51. Пароли технологического доступа (стандартные пароли «по умолчанию» компаний-производителей, предназначенные для доступа к системным ресурсам, серверам, ПО, СВТ, активному оборудованию передачи данных и других компонентов ИТ-инфраструктуры Общества) должны быть изменены или заблокированы сразу после завершения инсталляционных работ администратором данной ИС.

52. В случае компрометации личного пароля пользователя пароль должен быть немедленно заменен. Если пароль был утерян, то пользователю после выполнения его идентификации администратором ИС (системный администратор, администратор прикладных систем и т.п.) генерируется и выдается временный пароль взамен утерянного, который должен быть сменен сразу же при входе в систему.

53. В случае компрометации пароля администратора ИС (системного, сетевого администратора, администратора прикладных систем, администратора информационной безопасности и т.п.) пароль должен быть немедленно заменен.

7 Роли и ответственность

54. Контроль за выполнением требований и правил Политики возлагается на СП ИБ.

55. Ответственность за контроль исполнения и актуальность Политики, а также внесение в нее изменений возлагается на СП ИБ.

56. Ответственность за обеспечение должного исполнения требований и правил Политики возлагается на все заинтересованные СП в рамках их полномочий и в соответствии с положениями, установленными Политикой и разработанными на ее основе документами.

57. Руководители СП несут ответственность за своевременное доведение требований Политики до работников их подразделений и/или представителей третьих сторон в части их касающейся и за выполнение работниками их подразделений и/или представителями третьих сторон требований Политики.

58. Ответственность за организационное и методическое обеспечение процессов генерации, использования, смены и прекращения действия паролей, контроль действий пользователей при работе с паролями возлагается на СП ИБ и заинтересованные СП Общества.

59. Техническое обеспечение безопасности процессов генерации, использования, смены и прекращения действия паролей во всех СП Общества возлагается на администраторов ИС Общества.

60. Все пользователи должны быть ознакомлены с требованиями Политики.

61. Все пользователи ответственны за свои действия при использовании паролей в работе с ИС Общества и обращении с защищаемыми ИР Общества, а также за исполнение требований и правил, установленных Политикой и внутренними документами, разработанными на ее основе.

62. В случае выявления нарушений требований настоящей Политики пользователем ИС, которые повлекли или могли повлечь серьезный ущерб бизнес-деятельности Общества, должно инициироваться и вестись служебное расследование с привлечением заинтересованных СП и в соответствии с утверждённым Порядком расследования инцидентов ИБ.

63. Нарушение положений Политики или разработанных в поддержку Политики документов, включая любое преднамеренное действие, предпринимаемое с целью нарушить, блокировать или иным способом обойти установленные средства контроля в области ИБ, может привести к административному или уголовному наказанию в соответствии с действующим законодательством, а также НРД по управлению персоналом Общества.

64. Решение о применении и выборе мер ответственности принимается руководством Общества по результатам проведенного служебного расследования в зависимости от целесообразности применения рассматриваемых мер, а также от сведений об умышленности нарушения.